Université Mohammed Premier

Faculté des Sciences, Oujda

MASTER DE THÉORIE DES NOMBRES

Module M10

Discipline: MATHÉMATIQUES

Titre:

Théorie Analytique des Nombres.

préparé par :

Mohamed Talbi - Mohammed Taous

2019-2020

Table des matières

Table des matières **ii**

I Valuation ; Complétion ; Modules et Groupe de Classes de Rayon 1

1 Valuation et Complétion **2**
1.1 Valuations 2
1.1.1 Définitions et Propriétés 2
1.1.2 Places et Valuations 7
1.2 Complétion 9
1.3 Ramification dans les complétés 12
1.3.1 Lemme de Hensel 12
1.3.2 Ramification 13
1.4 Norme Local- Trace et Formule de produit 15

2 Groupe de classes de Rayon **19**
2.1 Généralités 19
2.1.1 Définitions 19
2.1.2 Théorème d'Approximation 22
2.2 Propriétés du groupe de Classes de Rayon 24

II Fonction zeta des corps de nombres ; $L-$fonction et Applications **27**

3 Fonction Zeta et $L-$Fonction **28**
3.1 Généralités 28
3.1.1 Séries de Dirichlet 28
3.1.2 Du Produits infinis aux séries 31

3.1.3 Prolongement de la fonction ζ de Riemman 33
3.1.4 Caractères dans les groupes abeliens 36
3.2 Fonction zeta de Dedekind (Sur un corps de nombres) 38
3.3 $L-$ series et Applications 41
3.3.1 Généralités sur la fonction L. 41
3.3.2 Applications aux corps quadratiques 44
3.3.3 Détermination de $L(1,\chi)$ 47
3.3.4 Exemples 50

4 Densité et Progression Arithmétique **52**
4.1 Densité 52
4.1.1 Définition et propriétés 52
4.1.2 propriétés 52
4.1.3 Densité des premiers dans le groupe de classes de rayon 53
4.2 Théorème de Densité de Frobenius 54
4.3 progression Arithmétique 58

Bibliographie **61**

Première partie

Valuation ; Complétion ; Modules et Groupe de Classes de Rayon

Chapitre 1

Valuation et Completion

1.1 Valuations

1.1.1 Définitions et Propriétés

Définition 1.1.1. Soit K un corps quelconque. La fonction $x \mapsto |x|$ de K dans $\mathbb{R}$ est dite valeur absolue sur K si les assertions suivantes sont vérifiées

i) $\forall x \in K$, $|x| \geq 0$ et $|x| = 0$ si et seulement si $x = 0$,

ii) $|xy| = |x||y|$ pour tout x,$y \in K$,

iii) Il existe une constante C tel que $|x + y| \leq C \max(|x|,|y|)$

Si de plus on a $|x| = 1$, pour tout $x \in K$, la fonction $x \mapsto |x|$ est dite la valeur absolue triviale.

Dans toute la suite du chapitre " **valeur absolue**" désigne " **valeur absolue non triviale**".

Exemples 1.1.1.

- La fonction $x \mapsto |x| = \sup(x, -x)$ de $\mathbb{R}$ dans $\mathbb{R}$ est une valeur absolue sur $\mathbb{R}$ (valeur absolue usuelle on la note $|\ |_{\mathbb{R}}$).
- La fonction $z = a + ib \mapsto |z| = \sqrt{a^2 + b^2}$ de $\mathbb{C}$ dans $\mathbb{R}$ est une valeur absolue sur $\mathbb{C}$ (module d'un nombre complexe).

Définition 1.1.2. Soient K un corps et $|\ |$ et $|\ |_1$ deux valeurs absolues définies sur K. On dit que $|\ |$ et $|\ |_1$ sont équivalentes si

$$\forall x \in K \text{ on a l'équivalence } \quad |x| < 1 \Leftrightarrow |x|_1 < 1$$

Proposition 1.1.1. *Soient K un corps et $|\ |$ et $|\ |_1$ deux valeurs absolues définies sur K. Alors $|\ |$ et $|\ |_1$ sont équivalentes si et seulement s'il existe $a \in \mathbb{R}$ tel que*

$$\forall x \in K \quad |x|_1 = |x|^a$$

Démonstration. Supposons que $|\ |$ et $|\ |_1$ sont équivalentes.
Puisque la valeur absolue $|\ |$ est non triviale, alors il existe $y \in K$ tel que $|y| > 1$. Soit $a = \frac{\ln|y|_1}{\ln|y|}$.
Pour x un élément non nul de K, il existe un nombre réel b tel que $|x| = |y|^b$.
Soit $\left(\frac{m_i}{n_i}\right)$ une suite de nombres rationnels (m_i et n_i des entiers avec $n_i > 0$) qui converge vers b de sorte que $b < \frac{m_i}{n_i}$. Alors $|x| = |y|^b < |y|^{\frac{m_i}{n_i}}$ et $|\frac{x^{n_i}}{y^{m_i}}| < 1$. Il s'ensuit de notre supposition que $|\frac{x^{n_i}}{y^{m_i}}|_1 < 1$ et $|x|_1 < |y|_1^{\frac{m_i}{n_i}}$, par passage à la limite, on tire que $|x|_1 \leq |y|_1^b$.
On obtient l'autre inégalité en considérant une suite $\left(\frac{m_i}{n_i}\right)$ qui converge vers b avec $b > \frac{m_i}{n_i}$. On conclut que $|x| = |y|^b \Rightarrow |x|_1 = |y|_1^b$. Donc pour tout $x \neq 0$, on déduit que $\frac{\ln|x|_1}{\ln|x|} = \frac{b\ln|y|_1}{b\ln|y|} = a$.
Donc $|x|_1 = |x|^a$. Or ceci est vrai pour $x = 0$. Donc pour tout $x \in K$ $|x|_1 = |x|^a$.
La réciproque est clair ($a > 0$). □

Remarque 1: Si une valeur absolue satisfait l'inégalité triangulaire

$$iv)\ \ |x+y| \leq |x| + |y| \ \ \text{(inégalité triangulaire)}$$

la constante C dans l'assertion $iii)$ peut prendre la valeur 2. Car $|x| + |y| \leq 2\max(|x|,|y|)$.

Définition 1.1.3. Soit K un corps quelconque et $x \mapsto |x|$ une valeur absolue définie sur K. Alors :

1. Si la valeur absolue $|\ |$ vérifie la condition $iv)$, (l'inégalité triangulaire), l' application $x \mapsto |x|$ est dite `valuation` sur K.

2. Si la constante C dans l'assertion $iii)$ peut prendre $C = 1$, la valeur absolue $|\ |$ est dite `valuation non archimidien`. C'est à dire, dans ce cas la valuation vérifie la condition

$$v)\ |x+y| \leq \max(|x|,|y|).$$

3. Une valuation sur K est dite `archimidien` s'elle n'est pas équivalente à aucune valuation vérifiant la condition $v)$.

Exercices

1. Soit K un corps admettant un plongement i de K dans $\mathbb{R}$, $i : K \to \mathbb{R}$. Soit $|x|_{\mathbb{R}}$ la valeur absolue usuelle définie sur $\mathbb{R}$. Montrer que l'application définie sur K par $y \mapsto |y| = |i(y)|_{\mathbb{R}}$ est une valuation archimidien.

2. Soit p un nombre premier. Montrer que toute valuation définie sur $\mathbb{Z}/p\mathbb{Z}$ est non archimidien.

Exemple de Valuation (Valuation $p-$adique)

Soit A un anneau de Dedekind et K son corps de fraction. Soit $\mathcal{P}$ un idéal premier non nul de A. Pour chaque élément $x \in A$, soit $v_{\mathcal{P}}(x)$ la puissance de $\mathcal{P}$ dans la factorisation de l'idéal $xA = (x)$ donnée par :

$$xA = \prod_{\mathcal{P} \text{ premier}} \mathcal{P}^{v_{\mathcal{P}}(x)}.$$

Si $x \neq 0$, $x \in K$ et pas nécessairement dans A, alors xA est un idéal fractionnaire et admet une factorisation en produit d'idéaux premiers de A. $v_{\mathcal{P}}(x)$ est définie pour tout x non nul de K.
Soit $A_{\mathcal{P}}$ le localisé de A en $\mathcal{P}$. Sans perte de généralité on écrit $\mathcal{P}$ pour l'idéal $\mathcal{P}A_{\mathcal{P}}$ de l'anneau à valuation discrète $A_{\mathcal{P}}$. On aura $xA_{\mathcal{P}} = \mathcal{P}^{v_{\mathcal{P}}(x)}$. Soit $\pi \in A_{\mathcal{P}}$ le générateur de l'idéal principal $\mathcal{P}$. Ainsi Chaque $x \in K$ peut s'exprimer come suit $x = u\pi^n$ avec n un entier et u une unité de $A_{\mathcal{P}}$ et on a :

$$n = v_{\mathcal{P}}(x) \text{ et } y = u\pi^{v_{\mathcal{P}}(x)} \tag{1.1}$$

Pour $x = 0$, on pose $v_{\mathcal{P}}(0) = +\infty$.

Propriétés

Soient x et y deux éléments non nuls de K. Alors

1. $v_{\mathcal{P}}(y)$ est un entier relatif,
2. $v_{\mathcal{P}}(xy) = v_{\mathcal{P}}(x) + v_{\mathcal{P}}(y)$,
3. $v_{\mathcal{P}}(x + y) \geq \min(v_{\mathcal{P}}(x), v_{\mathcal{P}}(y))$

Démonstration. Les assertions 1. et 2. se découlent immédiatement de la représentation donnée dans l'Équation 1.1.
Pour l'assertion 3.. Soit $x = u_1\pi^m$ et $y = u_2\pi^n$ avec u_1 et u_2 deux unités de $A_{\mathcal{P}}$. Supposons que $n \leq m$, alors $x + y = (u_2^{-1}u_1\pi^{m-n} + 1)u_2\pi^n$ et l'élément $u_2^{-1}u_1\pi^{m-n} + 1$ appartient à $A_{\mathcal{P}}$. Il s'ensuit que $v_{\mathcal{P}}(x + y) \geq n = \min(v_{\mathcal{P}}(x), v_{\mathcal{P}}(y))$. □

Définition 1.1.4. Toute fonction v qui satisfait les assertions $1., 2., 3.$ et la convention $v(0) = +\infty$, s'appelle `valuation exponentielle` sur K.

Remarque 2:

1. De toute valuation exponentielle v = $v_{\mathcal{P}}$ sur K, on obtient une valuation comme suit : Pour un nombre réel c, $0 < c < 1$, on pose $|x|_{v_{\mathcal{P}}} = c^{v_{\mathcal{P}}(x)}$. On vérifie facilement que les propriétés d'une valuation sont remplies. Aussi elle est non archimidien (pour le voir il suffit d'appliquer l'assertion 3.)
   La valuation $|\ |_{v_{\mathcal{P}}}$ s'appelle valuation $\mathcal{P}$-adique.

2. Si on remplace c dans $|x|_{v_{\mathcal{P}}}$ par un autre $c' \in]0,1[$, on obtient une autre valuation qui lui est équivalente.

Proposition 1.1.2. *Soient $|\ |$ une valuation non archimidien sur K, $A = \{x \in K \mid |x| \leq 1\}$ et $\mathcal{P} = \{x \in K \mid |x| < 1\}$. Alors :*

1. *A est un anneau local et $\mathcal{P}$ son idéal maximal et K son corps des fractions.*

2. *L'anneau A est un anneau de valuation discrète si et seulement si l'ensemble $\{|x|, x \in K, x \neq 0\}$ est un sous groupe multiplicative isomorphe à $(\mathbb{Z},+)$.*

Démonstration. 1. Montrons que A est un anneau. Pour x,$y \in A$ on a

$$|xy| = |x||y| \leq 1 \text{ et } |x+y| \leq \max(|x|,|y|) \leq 1. \tag{1.2}$$

Donc xy et $x+y$ appartiennent à A. Or $|-1|^2 = |(-1)^2| = |1| = 1$ donc $|-1| = |1|$ d'où $|-y| = |y|$, ainsi $x - y \in A$. Par conséquence A contient l'identité de K.
Pour chaque $z \in K$ avec $z \neq 0$, on a $|z||z^{-1}| = 1$, donc $|z| \leq 1$ ou bien $|z^{-1}| \leq 1$, implique que $z \in A$ ou $z^{-1} \in A$, d'où K est le corps des fractions de A.
On a $\mathcal{P} \subset A$ et $1 \in A$ mais $1 \notin \mathcal{P}$. On vérifie simplement en utilisant l'Équation (1.2) que $(\mathcal{P},+)$ est un sous groupe de $(A,+)$ et que $\forall x \in A$, et $a \in \mathcal{P}$ on a ax et xa appartiennent à $\mathcal{P}$. C'est à dire que $\mathcal{P}$ est un idéal de A.
Montrons que $\mathcal{P}$ est un idéal maximal de A. Soit $x \in A$ tel que $x \notin \mathcal{P}$, alors $|x| = 1$ implique que $|x^{-1}| = 1$, d'où $x^{-1} \in A$. Par conséquence x est une unité de A. Si I un idéal de A différent de A, alors $I \subset \mathcal{P}$ car I ne peut pas contenir des éléments qui n'appartiennent pas à $\mathcal{P}$, sinon il contient une unité de A et donc il coincide avec A. D'où $\mathcal{P}$ est le seul idéal maximal de A, par conséquence A est local.

2. On suppose que A est un anneau de valuation discrète, soit $\mathcal{P} = \pi A$ son idéal maximal. Alors $\forall x \in K^*,\ x = \epsilon\pi^n$, $n \in \mathbb{Z}$, avec ϵ une unité de A.
   $|x| = |\epsilon||\pi^n|$, or $|\epsilon| = 1$, car sinon $\epsilon \in \mathcal{P}$ et donc $\mathcal{P} = A$ ce qui est impossible, donc $|x| = |\pi^n|$. On pose $c = |\pi|$ donc $|K^*| = \{c^n \,|\, n \in \mathbb{Z}\}$, d'où $|K^*|$ est un sous groupe

multiplicatif isomorphe à $(\mathbb{Z},+)$.

Maintenant supposons qu'il existe un isomorphisme $\varphi : |K^*| \to (\mathbb{Z},+)$, d'où il existe $z \in K^*$ tel que $\varphi(|z|) = 1$ et $\varphi(|z^{-1}z|) = \varphi(1) = 0$, soit $\varphi(|z^{-1}|) + \varphi(|z|) = 0$ ainsi $\varphi(|z^{-1}|) = -\varphi(|z|)$. On peut toujours choisir φ de sorte que $z \in A$, car si $z \notin A$, alors $z^{-1} \in A$ et $\varphi(|z^{-1}|) = -1$. On prend $\varphi' = -\varphi$ et on a $\varphi'(|z^{-1}|) = 1$ et $z^{-1} \in A$. Donc $\forall n \in \mathbb{N}$, $\varphi(|z|^n) = n$ et $z^n \in A$, d'où $\mathbb{N} \subset \varphi(|A|)$. D'autre part, par hypothèse, on a $z^{-1} \notin A$, soit $z^{-1} \in K \setminus A$, $\varphi(|z^{-1}|) = -1$ et si $n \in \mathbb{N}$ on a $\varphi(|z^{-n}|) = -n$ donc $\mathbb{Z}^- \subset \varphi(|K \setminus A|)$. Comme $A \cap K \setminus A = \emptyset$ alors $\varphi(|A|) \cap \varphi(|K \setminus A|) = \emptyset$. D'où $\mathbb{N} = \varphi(|A|)$ et $\mathbb{Z}^- = \varphi(|K \setminus A|)$, par suite $\forall x \in A$, $\exists n \in \mathbb{N} \mid \varphi(|x|) = n = \varphi(|z^n|)$ d'où $|x| = |z^n|$ ce qui implique que $|xz^{-n}| = 1$ c'est à dire xz^{-n} est une unité de A. Donc $x = \epsilon z^n$ où ϵ est une unité de A. De même pour tout x appartient à $K \setminus A$, il existe une unité ϵ de A tel que $x = \epsilon z^n$ avec $n \in \mathbb{Z}$. On vérifie facilement que zA est le seul idéal maximal de A et que tout idéal de A est principal. Par suite A est un anneau de valuation discrète.

□

Proposition 1.1.3. *Soient K un corps et $|\ |$ une valuation définie sur K. Alors $|\ |$ est non archimidien si et seulement si l'ensemble $\{|n1_K|,\ n \in \mathbb{Z}\}$ est borné.*

Démonstration. $\Rightarrow$) Si $|\ |$ est non archimidien, alors pour tout entier $n \in \mathbb{N}$ on a $|n1_K| = |1 + 1 + \ldots + 1| \leq |1|$. Donc $\{|n1_K|,\ n \in \mathbb{Z}\}$ est borné.
$\Leftarrow$) Supposons qu'il existe $N \in \mathbb{R}$ tel que $\forall n \in \mathbb{N},\ |n1_K| \leq N$. On a

$$|x + y|^n \leq \sum_{k=0}^{n} |\binom{n}{k}.1||x|^{n-k}|y|^k$$

or $|\binom{n}{k}.1| \leq N$. Si On suppose que $\max(|x|,|y|) = |x|$, alors on en déduit que

$$|x + y|^n \leq \sum_{k=0}^{n} |N|x|^n = N(n+1)|x|^n.$$

Donc $|x+y| \leq N^{\frac{1}{n}}(n+1)^{\frac{1}{n}}|x|$, par passage à la limite on trouve que $|x+y| \leq |x| = \max(|x|,|y|)$.

□

Proposition 1.1.4. ***(Détermination des valuations de** $\mathbb{Q}$**)***

1. *Toute valuation non archimidien de $\mathbb{Q}$ est équivalente à une valuation $p-$adique où p un nombre premier.*

2. *Toute valuation archimidien de $\mathbb{Q}$ est équivalente à une valuation restriction d'une ordinaire valeur absolue sur $\mathbb{R}$.*

Démonstration. Voir TD □

1.1.2 Places et Valuations

Définition 1.1.5. Soit K un corps. On définit les places de K comme suit :

1. Une classe d'équivalence des valuations sur K s'appelle **premier de** K (ou **place de** K).

2. Une classe d'équivalence des valuations archimidien s'appelle **premier infini** (ou **place infinie**) de K. Et une classe d'équivalence des valuations non archimidien s'appelle **premier fini** (ou **place finie**).

On note par $\mathcal{B}$ (ou $\mathcal{P}$) les premiers de K et la valuation dans $\mathcal{B}$ est notée par $|\ |_{\mathcal{B}}$ et sa valeur en un élément $x \in K$ est $|x|_{\mathcal{B}}$.

Remarque 3: Les valuations de $\mathbb{Q}$ proviennent des premiers de $\mathbb{Q}$ qui correspondent aux nombres premiers et un premier infini (pour les valuations archimidien).

Soit p un nombre premier et $\mathcal{P}$ le premier de $\mathbb{Q}$ qui correspond à la valuation $p-$adique. Soit $|\ |_{\mathcal{P}}$ la valuation dans $\mathcal{P}$ qui satisfait $|p|_{\mathcal{P}} = \frac{1}{p}$. Et soit $\mathcal{P}_\infty$ le premier infini et $|\ |_\infty$ l'usuelle valeur absolue définie par $|x|_\infty = \begin{cases} x, & \text{si } x > 0; \\ -x, & \text{si } x \leq 0. \end{cases}$

Les valuations ainsi définie s'appellent les **valuations normalisées**.

Proposition 1.1.5. *Soit $\mathcal{P}$ un premier de $\mathbb{Q}$ et Soit $|x|_{\mathcal{P}}$ la valuation normalisée dans le premier $\mathcal{P}$. Alors pour chaque x non nul de $\mathbb{Q}$ on a*

$$\prod_{\mathcal{P}\ premier} |x|_{\mathcal{P}} = 1,$$

où $\mathcal{P}$ parcourt tous les premiers de $\mathbb{Q}$.

Démonstration. La fonction $\Pi(x) = \prod_{\mathcal{P}\ \text{premier}} |x|_{\mathcal{P}}$ est bien définie. Car pour chaque x, il existe uniquement un nombre fini de premier $\mathcal{P}$ pour les quels $|x|_{\mathcal{P}} \neq 1$, à savoir le premier infini et les premiers qui correspondent aux nombres premiers divisant soit le dénominateur soit le numérateur de x. Puisque chaque valuation est multiplicative on remarque que $\Pi(xy) = \Pi(x)\Pi(y)$. Il suffit donc de montrer que $\Pi(p) = 1$ pour tout nombre premier. Or ceci est clair car $\Pi(p) = |p|_\infty |p|_p = p \times \frac{1}{p} = 1$. □

Décomposition des premiers infinis d'un corps de nombres

D'après le théorème d'Ostroski, toute classe de valuations archimidien définies sur un corps de nombres est complètement déterminée par un plongement de K dans $\mathbb{R}$ ou $\mathbb{C}$. Les premiers infinis réels correspondent aux classes de valuations données par les différentes plongements de K dans $\mathbb{R}$, et les premiers infinis complexes correspondent aux classes de valuations données par les différentes paires conjugués des plongements de K dans $\mathbb{C}$.
Soient L une extension finie de K de degré g, $g = [L : K]$, et $\mathcal{P}$ un premier infini de K. On décrit toutes les extensions de $\mathcal{P}$ dans L.

1. Soient $\mathcal{P}$ un premier infini complexe et τ un plongement de K dans $\mathbb{C}$ qui correspond à $\mathcal{P}$. Puisque $\mathbb{C}$ est algébriquement clos, on sait par la théorie de Galois qu'il existe $g = [L : K]$ plongement τ_i de L dans $\mathbb{C}$ tel que $\tau_i(x) = \tau(x)$ pour tout $x \in K$. Ces derniers sont différents et donc représentent g premiers infinis complexes, notés $\mathcal{B}_1, \cdots, \mathcal{B}_g$.
   On écrit formellement
   $$\mathcal{P} = \mathcal{B}_1 .... \mathcal{B}_g,$$
   et on a pour tout i, $1 \leq i \leq g$, l'indice de ramification e_i et le degré résiduel f_i valent 1. De plus on a l'égalité
   $$[L : K] = \sum_{i=1}^{g} e_i f_i.$$

2. Soient $\mathcal{P}$ un premier infini réel et τ un plongement de K dans $\mathbb{R}$ qui correspond à $\mathcal{P}$. D'après la théorie de Galois, il existe $[L : K]$ extensions de τ à L, certains d'eux leurs images sont contenus dans $\mathbb{R}$ et les autres sont en nombres paires conjugués et leurs images sont contenus dans $\mathbb{C}$.
   On écrit $\tau_1, \cdots, \tau_a, \tau_{a+1}, \cdots, \tau_{a+b}, \overline{\tau_{a+1}}, \cdots, \overline{\tau_{a+b}}$, où $\tau_i(L) \subset \mathbb{R}$ pour i, $1 \leq i \leq a$. Donc on a $a + 2b = [L : K]$.
   On écrit formellement
   $$\mathcal{P} = \mathcal{B}_1 .... \mathcal{B}_a . \mathcal{B}_{a+1}^2 .... \mathcal{B}_{a+b}^2.$$
   On a les indices de ramification et les degrés résiduels des extensions réels de $\mathcal{P}$ valent 1, mais les indices de ramification des extensions complexes de $\mathcal{P}$ valent 2 et leurs degrés résiduels valent 1. De plus on a l'égalité
   $$[L : K] = \sum_{i=1}^{g} e_i f_i.$$

1.2 Complétion

Soit $|\ |$ une valuation sur K. Une suite (a_n) des éléments de K est dite suite de Cauchy si pour chaque nombre réel positif ϵ, il existe $N \in \mathbb{N}$ tel que

$$|a_n - a_m| < \epsilon, \quad \forall n,m \geq N.$$

Notons qu'une suite de Cauchy dans K peut ne pas converger vers un élément de K. Par exemple : $u_n = \sum_{k=0}^{n} \frac{1}{k!}$ est une suite des éléments de $\mathbb{Q}$ qui converge vers e, pour la valeur absolue $|\ |_\infty$ mais $e \notin \mathbb{Q}$.

Définition 1.2.1. Un corps K est dit complet pour une valuation si toute suite de Cauchy converge, pour cette valuation, vers un élément de K.

Soit K un corps muni d'une valuation $|\ |$, $\mathcal{C}$ l'ensemble des suites de Cauchy et $\mathcal{C}_0$ l'ensemble des suites de Cauchy qui convergent vers 0. Alors $\mathcal{C}$ est un anneau et $\mathcal{C}_0$ est un idéal maximal de $\mathcal{C}$. On pose $\widehat{K} = \mathcal{C}/\mathcal{C}_0$, on a $\widehat{K}$ est un corps. On fait plonger K dans $\widehat{K}$ de la façon suivante : Soit $\alpha \in K$, alors $(\alpha, \ldots, \alpha, \ldots)$ est une suite de cauchy. On identifie l'élément α avec la classe de la suite ainsi définie.
On dit que $K \subset \widehat{K}$, et on définit une valuation sur $\widehat{K}$ par : Si $\overline{(a_n)} \in \widehat{K}$, on pose $|\overline{(a_n)}| = \lim_{n\to\infty} |a_n|$. On vérifié immédiatement que l'application ainsi définie sur $\widehat{K}$ est une valuation sur $\widehat{K}$, et que si la valuation définie sur K est non archimidien, alors elle est non archimidien. Aussi $(\widehat{K},|\ |)$ est complet.

Proposition 1.2.1. *Soient K et L deux corps munis des valuations $|\ |$ et $|\ |_1$ respectivement. On suppose qu'il existe un plongement $\sigma : K \to L$ tel que $|\sigma(x)|_1 = |x|$ pour tout $x \in K$. Soit $(\widehat{K},|\ |,i)$ le complété de $(K,|\ |)$ et $(\widehat{L},|\ |_1,i_1)$ le complété de $(L,|\ |_1)$. Alors il existe un unique plongement $\widehat{\sigma} : \widehat{K} \to \widehat{L}$ de sorte que le diagramme suivant soit commutatif et $|\widehat{\sigma}(z)|_1 = |z|$ $\forall z \in \widehat{K}$.*

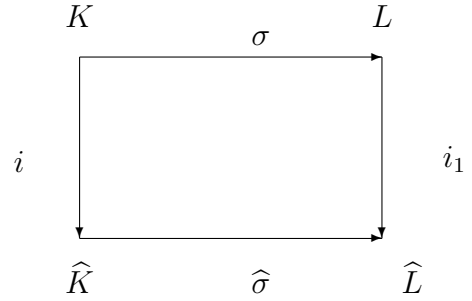

FIGURE 1.1 : Diagramme 1

Démonstration. Pour définir $\widehat{\sigma}$, pour un élément $a \in \widehat{K}$, soit (a_n) la suite de Cauchy des éléments de K tel que $a = (a_n) + \mathcal{C}_0$ dans $\mathcal{C}/\mathcal{C}_0$. Alors la suite $\sigma(a_n)$ est une suite de Cauchy de L (Par hypothèse). Donc $(i_1(\sigma(a_n)))$ est une suite de Cauchy dans $\widehat{L}$ qui converge vers un élément $b \in \widehat{L}$.
Définissons $\widehat{\sigma}$ par : $\widehat{\sigma}(a) = \lim\limits_{n\to\infty} i_1(\sigma(a_n)) = b$. On vérifie facilement que $\widehat{\sigma}$ est bien définie et conserve les valuations.
Montrons que c'est unique. Soit Θ un autre plongement de $\widehat{K}$ dans $\widehat{L}$ de sorte que le Diagramme FIGURE1.1 soit commutatif et conserve les valuations. Alors avec a et (a_n) ainsi définies on a

$$\Theta(a) = \lim_{n\to\infty} \Theta(i(a_n)) = \lim_{n\to\infty} i_1(\sigma(a_n)) = \widehat{\sigma}(a).$$

Ce qui montre l'unicité de l'extension de σ. □

Corollaire 1.2.1. *Soient K un corps et $|\ |$ une valuation sur K. Alors le complété $(\widehat{K},|\ |)$ de $(K,|\ |)$ est unique à isomorphisme près qui préserve les valuations.*

Démonstration. Dans la **Proposition**1.2.1 on prend $L = K$ et $\sigma = id_K$. Si $(\widehat{K},|\ |)$ et $(\widehat{K}_1,|\ |)$ sont deux complétés de $(K,|\ |)$, il existe deux homomorphismes $\sigma_1 : \widehat{K} \to \widehat{K}_1$ et $\sigma_2 : \widehat{K}_1 \to \widehat{K}$ qui préservent les valuations et vérifient $(\sigma_1\sigma_2)_{|K} = id_K$ et $(\sigma_2\sigma_1)_{|K} = id_K$. L'identité sur $\widehat{K}$ et sur $\widehat{K}_1$ ont aussi cette propriété et par l'unicité on a $\sigma_1\sigma_2 = id_{\widehat{K}_1}$ et $\sigma_2\sigma_1 = id_{\widehat{K}}$. Il s'ensuit que σ_1 et σ_2 sont des isomorphismes. □

Exemple 1.2.1.

- Le complété de $(\mathbb{Q},|\ |_\infty)$ est noté $\mathbb{Q}_\infty$ et il est isomorphe à $\mathbb{R}$.
- Le complété de $(\mathbb{Q},|\ |_p)$ est noté $\mathbb{Q}_p$ et s'appel le corps des nombres $p-$adique.

Proposition 1.2.2. *Soient K un corps muni d'une valuation non archimidien $|\ |$, $\widehat{K}$ son complété, $A = \{x \in K \,|\, |x| \leq 1\}$, $\widehat{A} = \{x \in \widehat{K} \,|\, |x| \leq 1\}$, $\mathcal{P} = \{x \in K \mid |x| < 1\}$ et $\widehat{\mathcal{P}} = \{x \in \widehat{K} \mid |x| < 1\}$. Alors :*
Si A est un anneau de valuation discrète , il en est de même $\widehat{A}$. De plus il existe $\pi \in A$ tel que $P = \pi A$ et $\widehat{P} = \pi\widehat{A}$.

Démonstration. On suppose que A est un anneau de valuation discrète, alors $|K^*|$ est un sous groupe multiplicatif de $(\mathbb{R}^*,\times)$ isomorphe à $(\mathbb{Z},+)$. Soit $\alpha \in \widehat{K}^*$, alors $|\alpha| = \lim\limits_{n\to\infty}(|a_n|)$ où (a_n) est une suite de Cauchy à valeurs dans K. Écrivons $a_n = \epsilon\pi^{r_n}$ avec ϵ est une unité de A et $r_n \in \mathbb{Z}$. Donc $|a_n| = |\pi|^{r_n} = c^{r_n}$ où $c = |\pi| < 1$.
L'ensemble $\{r_n \,|\, n \in \mathbb{N}\}$ doit être fini car sinon la limite vaut 0, donc $|\alpha| = \lim\limits_{n\to\infty} c^{r_n} = c^k$ car r_n est constante à partir d'un certain rang. Donc $|\alpha| = |a_N|$ pour un certain rang N assez grand. Par suite $|\widehat{K}^*| \subset |K^*|$, d'où $|\widehat{K}^*| = |K^*|$. Donc le sous groupe $(|\widehat{K}^*|,\times)$ est égal à $(|K^*|,\times)$ qui

est isomorphe à $(\mathbb{Z},+)$. Ce qui démontre que $\widehat{A}$ est un anneau de valuation discrète.
On suppose que $P = \pi A$ et $\widehat{\mathcal{P}} = x\widehat{A}$ donc $|\pi| = c$ et $|x| = c^s$, par suite $|\pi^s| = |x|$ implique que $|\pi^s x^{-1}| = 1$ d'où $\pi^s x^{-1}$ est une unité. Donc $x = \epsilon^{-1}\pi^s$ et $x\widehat{A} = \pi^s\widehat{A} \subset \pi\widehat{A}$ d'où $s = 1$. Il s'ensuit que $x\widehat{A} = \pi\widehat{A}$. Enfin $\widehat{\mathcal{P}} = \pi\widehat{A}$. □

Remarque 4:

- Si A est un anneau de valuation discrète, alors $\forall\alpha \in \widehat{K}$, il peut s'écrire sous la forme $\alpha = (a_n)$ où $|a_n|$ est constante pour tout $n \in \mathbb{N}$. Car si $(b_n) \in \overline{(a_n)} = \alpha$, alors $|b_n|$ est constante à partir d'un certain rang N, par suite si on pose

$$\begin{cases} c_n = b_n, & \text{si } n \geq N \\ c_n = b_N, & \text{si } n \leq N. \end{cases}$$

  On a $c_n \in \overline{(a_n)} = \alpha$ et $|c_n|$ est constante.

- $\alpha \in \widehat{A}$ est une unité de $\widehat{A}$ si et seulement si $\alpha = (a_n)$ avec $|a_n| = 1$, $\forall n \geq 0$.

Proposition 1.2.3. *On garde les mêmes notations et hypothèses de la* ***Proposition****1.2.2 Alors on a :*

$$A/\mathcal{P} \simeq \widehat{A}/\widehat{\mathcal{P}}.$$

Démonstration. Soit $\alpha \in \widehat{A}$ et $\alpha \notin \widehat{\mathcal{P}}$, alors α est une unité de $\widehat{A}$, il existe donc une suite (a_n) des éléments de A tel que $|a_n| = 1$ qui converge vers α. Donc il existe $N \in \mathbb{N}$ tel que $|a_{n+1} - a_n| < 1/2$, $\forall n \geq N$. On peut supposer que $\forall n \geq 1$, $|a_{n+1} - a_n| < 1/2$, donc $a_{n+1} - a_n \in \widehat{\mathcal{P}}$. Par suite

$$\begin{aligned} a_{n+1} &\equiv a_n \bmod \widehat{\mathcal{P}} \\ &\vdots \\ a_2 &\equiv a_1 \bmod \widehat{\mathcal{P}} \end{aligned}$$

Ce qui implique que pour tout $n \in \mathbb{N}$ on a $a_n \equiv a_1 \bmod \widehat{\mathcal{P}}$.
Soit $\alpha_0 = \overline{(a)}$ où $a = a_1$, donc $\alpha - \alpha_0 \in \widehat{\mathcal{P}}$, c'est à dire $\alpha \equiv \alpha_0 \bmod \widehat{\mathcal{P}}$. Or α_0 s'identifie à a_1. Donc $\alpha \in a_1 + \widehat{\mathcal{P}}$. Il s'ensuit que $\widehat{A} = A + \widehat{\mathcal{P}}$.
Donc

$$\widehat{A}/\widehat{\mathcal{P}} \simeq A + \widehat{\mathcal{P}}/\widehat{\mathcal{P}} \simeq A/A \cap \widehat{\mathcal{P}} \simeq A/\mathcal{P}$$

□

Proposition 1.2.4. *On garde les mêmes notations et hypothèses de la* ***Proposition****1.2.1 et la* ***Proposition****1.2.2. Alors on a :*

Tout élément α de $\widehat{K}$ s'écrit sous la forme suivante $\alpha = \pi^r (s_0 + s_1\pi + s_2\pi^2 + \ldots)$ où $s_i \in S$, avec S un système de représentants de $A/\mathcal{P} \simeq \widehat{A}/\widehat{\mathcal{P}}$

Démonstration. Soit $\alpha \in \widehat{K}$ alors $\alpha = \epsilon\pi^r$ où ϵ est une unité et $r \in \mathbb{Z}$. On a $\epsilon \in \widehat{A}$, donc $\overline{\epsilon} = \overline{s_0}$ où $s_0 \in S$, d'où $\epsilon - s_0 = \pi x_1$ où $x_1 \in \widehat{A}$. Aussi comme $x_1 \in \widehat{A}$, il existe $s_1 \in S$ tel que $\overline{x_1} = \overline{s_1}$ ce qui implique $x_1 - s_1 = \pi x_2$ et donc $\epsilon - s_0 = \pi x_1 = s_1\pi + \pi^2 x_2$ ce qui entraîne que $\epsilon - s_0 - s_1\pi = \pi^2 x_2$. Si on répète l'opération $i+1$ fois on trouve :

$$\epsilon - s_0 - s_1\pi - s_2\pi^2 - \ldots - s_i\pi^i = \pi^{i+1}x_{i+1} \text{ avec } x_{i+1} \in \widehat{A}$$

Or $|\pi^{i+1}x_{i+1}| \leq c^{i+1} \to 0$ donc la suite $s_0 + s_1\pi + s_2\pi^2 + \ldots + s_n\pi^n$ converge vers ϵ lorsque n tend vers l'infini et cette limite est donnée par $\sum_{i\geq 0} s_k\pi^k$. Par conséquence

$$\alpha = \pi^r \left(s_0 + s_1\pi + s_2\pi^2 + \ldots + s_n\pi^n + \ldots\right)$$

. □

Exemple 1.2.2. Soit $\mathbb{Z}_{(3)}$ le localisé de $\mathbb{Z}$ en (3) et $\mathbb{Q}_3$ le complété de $\mathbb{Q}$ pour la valuation 3−adique. Donc $S = \{0,1,2\}$ est un ensemble de $\mathbb{Z}_{(3)}/3\mathbb{Z}_{(3)}$. Donc chaque élément de $\mathbb{Q}_3$ s'écrit sous la forme suivante : $3^r (s_0 + 3s_1 + 3^2 s_2 + \ldots)$ avec $s_i \in \{0,1,2\}$.
Par exemple :
$-\frac{1}{8} = \frac{1}{1-3^2} = 1 + 3^2 + 3^4 + \ldots$,
$-1 = \frac{2}{1-3} = 2 + 2.3 + 2.3^2 + \ldots$.

1.3 Ramification dans les complétés

1.3.1 Lemme de Hensel

Dans toute la suite de ce chapitre la proposition A **est AVD complet** signifie que A **est un anneau de valuation discrète dont le corps des fractions est complet pour la valuation non archimidien dont A est l'anneau des valuations.**
Soit $\mathcal{P}$ l'unique idéal maximal de A, le Lemme de Hensel consiste à trouver le lien entre la factorisation des polynômes dans $A[X]$ et celle dans $\overline{A}[X]$, où $\overline{A}$ est le corps résiduel de A modulo l'idéal $\mathcal{P}$.

Proposition 1.3.1. *(Lemme de Hensel) On suppose que A est AVD Complet et $\overline{A}$ son corps résiduel. Supposons que $F(X)$ est un polynôme unitaire de $A[X]$ tel que son image $\overline{F}(X)$ dans $\overline{A}[X]$ admet la factorisation suivante $\overline{F}(X) = g(X)h(X)$ avec $g(X)$ et $h(X)$ premiers entre*

eux. Alors $F(X) = G(X)H(X)$ avec $G(X)$ et $H(X)$ des polynômes de $A[X]$ ayant les mêmes degrés que $g(X)$ et $h(X)$ et $\overline{G}(X) = g(X)$ et $\overline{H}(X) = h(X)$.

Démonstration. Soit $R = A[X]/(F(X))$. Puisque F est unitaire, alors l'algèbre R admet un nombre fini de générateur. On admet que R est un $A-$module libre complet et de valuation discrète (Pour la preuve on suit les mêmes démarches que dans [Théorème 3.3, Page 103, [1]]). Soit $\mathcal{P}$ l'idéal maximal de A. Alors :

$$R/\mathcal{P}R \simeq \overline{A}[X]/(g(X)h(X)) \simeq \overline{A}[X]/(g(X)) \oplus \overline{A}[X]/(h(X))$$

Soient e_1 et e_2 les éléments identités de chaque composante. Écrivons $e_1 = (1,0)$ et $e_2 = (0,1)$. Donc les éléments e_i sont idempotent et $e_1e_2 = 0$, alors il existe des éléments idempotent E_1 et E_2 dans R tel que $E_i + \mathcal{P}R = e_i$ et $E_1E_2 = 0$ [Théorème 3.2, page 102, [1]]. IL s'ensuit que $R = RE_1 \oplus RE_2$ et $RE_1/\mathcal{P}RE_1 \simeq \overline{A}[X]/(g(X))$ et $RE_2/\mathcal{P}RE_2 \simeq \overline{A}[X]/(h(X))$. Soit x l'image de X dans R. Le polynôme caractéristique de x opérant sur R est $F(X)$. Soit $G(X)$ et $H(X)$ les polynômes caractéristiques de x opérant sur RE_1 respectivement sur RE_2. Alors $F(X) = G(X)H(X)$. Après réduction modulo $\mathcal{P}$, on remarque que $\overline{G}(X)$ est celui de x sur $\overline{RE_1}$ qui est isomorphe en tant qu'un $R-$module à $\overline{A}[X]/(g(X))$. Si $g(X)$ n'est pas unitaire. Soit $a \in A$ une unité tel que $\overline{a}$ le coefficient dominant de $g(X)$. Donc le polynôme caractéristique de x sur $\overline{RE_1}$ est $\overline{a}^{-1}g(X)$. Il s'ensuit que $\overline{G}(X) = \overline{a}^{-1}g(X)$ et donc $aG(X)$ est le polynôme dans $A[X]$ qui est congru à $g(X)$ mod $\mathcal{P}$. Puisque $F(X) = aG(X) \times a^{-1}H(X)$ on obtient la factorisation de F. □

Corollaire 1.3.1. *On garde les mêmes notations et hypothèses de la* ***Proposition****1.3.1. Supposons que $F(X)$ admet une racine de multiplicité* 1 *dans $\overline{A}$, alors $F(X)$ admet une racine de multiplicité* 1 *dans A.*

Démonstration. Si $\overline{F}(X) = (x - \overline{a})h(X)$ avec $h(\overline{a}) \neq 0$, alors ces facteurs sont premiers entre eux. Donc $F(X)$ admet un facteur de degré 1 qui est premier à l'autre facteur. □

Exemple 1.3.1. Le polynôme $X^{p-1} - 1$ admet $p - 1$ racine distincts dans $\mathbb{Q}_p$.
En effet : Soit $\mathbb{Z}_p$ l'anneau de la valuation $p-$adique sur $\mathbb{Q}_p$, alors $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$ est le corps à p éléments. Donc modulo p le polynôme $X^{p-1} - 1$ admet $p - 1$ racines distincts. Donc par le **Corollaire**1.3.1, on conclut qu'il admet aussi $p - 1$ racine différentes dans $\mathbb{Z}_p$.

1.3.2 Ramification

Soit K un corps de nombres, A l'anneau dont le corps des fractions est K. On suppose que A est un anneau de valuation discrète et $\mathcal{P}$ son idéal maximal. Soit L une extension finie de K et A' la clôture intégrale de A dans L. la factorisation de $\mathcal{P}A'$ est donnée par :

$$\mathcal{P}A' = \mathcal{B}_1^{e_1} \dots \mathcal{B}_g^{e_g}, \tag{1.3}$$

avec $\mathcal{B}_i^{e_i}$ des premiers différents dans A'.
Soit $\mathcal{B} = \mathcal{B}_i$, $i \in \{1 \dots g\}$, et soient la valuation $|\ |_{\mathcal{P}}$ la valuation $\mathcal{P}-$adique de K et $|\ |_{\mathcal{B}}$ la valuation $\mathcal{B}-$adique de L. On suppose que pour tout $x \in K$ on a $|x|_{\mathcal{P}} = |x|_{\mathcal{B}}$. Soit $K_{\mathcal{P}}$ et $L_{\mathcal{B}}$ les complétés de K et L pour $|\ |_{\mathcal{P}}$ et $|\ |_{\mathcal{B}}$ respectivement et $\widehat{A}$ et $\widehat{A}'$ les anneaux AVD Complet associées et $\widehat{\mathcal{P}}$ et $\widehat{\mathcal{B}}$ leurs idéaux maximaux respectivement.

Théorème 1.3.1. *Avec les conditions ci-dessus on a les propriétés suivantes*

1. $\widehat{\mathcal{P}} = \mathcal{P}\widehat{A},\ \widehat{\mathcal{B}} = \mathcal{B}\widehat{A}'$
2. $e(\widehat{\mathcal{B}}/\widehat{\mathcal{P}}) = e(\mathcal{B}/\mathcal{P})$*(égalité des indices de ramification)*
3. $f(\widehat{\mathcal{B}}/\widehat{\mathcal{P}}) = f(\mathcal{B}/\mathcal{P})$ *(égalité des degrés résiduels)*
4. $[L_{\mathcal{B}} : K_{\mathcal{P}}] = ef$

Démonstration. Par la **Proposition**1.2.1 $\mathcal{P}$ et $\widehat{\mathcal{P}}$ peuvent être engendré par le même élément de A, de même pour $\mathcal{B}$ et $\widehat{\mathcal{B}}$ dans A'. Donc l'assertion 1. est vérifiée.
Si $\mathcal{B} = \mathcal{B}_i$ dans la factorisation (Equation1.3), alors pour tout $i \neq j$ on a $\mathcal{B}_j\widehat{A}' = \widehat{A}'$. Car $\widehat{A}'$ est un anneau de valuation discrète et $\mathcal{B}_j$ contient un élément qui n'appartient pas à $\mathcal{B}_i$, qui est forcement une unité dans $\widehat{A}'$. Alors

$$\widehat{\mathcal{P}}\widehat{A}' = (\mathcal{P}A')\widehat{A}' = (\mathcal{B}_1^{e_1} \dots \mathcal{B}_g^{e_g})\widehat{A}' = \left(\mathcal{B}_i\widehat{A}'\right)^{e_i} = \widehat{\mathcal{B}}_i^{\,e_i}$$

ce qui entraîne la deuxième assertion.
La troisième se découle de la **Proposition**1.2.3.
Pour la dernière assertion, remarquons que $[L_{\mathcal{B}} : K_{\mathcal{P}}]$ est finie. Car chaque base de L sur K est un ensemble générateur de $L_{\mathcal{B}}$ sur $K_{\mathcal{P}}$ et on suit les mêmes démarches du[Théorème 6.6, page 30,[1]] on obtient le résultat. □

Soit K un corps de nombres, A l'anneau des entiers algébriques, $\mathcal{P}$ un idéal premier non nul de A et p le nombre premier dans $\mathcal{P}$. Soit $\overline{A} = A/\mathcal{P} \simeq \mathrm{GF}(p)$.

Théorème 1.3.2. *Soit $\widehat{L}$ une extension de dimension finie du complété $K_{\mathcal{P}}$ tel que $\widehat{\mathcal{P}}$ est non ramifié dans $\widehat{L}$ et Soit $f = [\widehat{L} : K_{\mathcal{P}}]$. Alors $\widehat{L} = K_{\mathcal{P}}(\beta)$ où β est une racine $p^f - 1$ primitive de l'unité. Inversement, pour tout entier positif f et une racine $p^f - 1$ primitive de l'unité β, l'extension $K_{\mathcal{P}}(\beta)$ est non ramifiée et de degré f.*

Démonstration. Soit $\widehat{A}$ l'anneau de valuation dans $K_{\mathcal{P}}$ et $\widehat{S}$ sa clôture intégrale dans $\widehat{L}$. L'hypothèse sur la ramification (non ramification) entraîne que $\widehat{\mathcal{P}}\widehat{S}$ est l'idéal maximal de $\widehat{S}$ et $\widehat{S}/\widehat{\mathcal{P}}\widehat{S} \simeq \mathrm{GF}(p^f)$ et $\widehat{A}/\widehat{\mathcal{P}}\widehat{A} \simeq \mathrm{GF}(p)$. Donc $\widehat{S}/\widehat{\mathcal{P}}\widehat{S}$ contient une racine primitive $p^f - 1$ de l'unité. Par le Lemme de Hensel (**Proposition**1.3.1), il existe une racine $p^f - 1$ primitive de l'unité β qui appartiennent à $\widehat{S}$. L'anneau $\widehat{A}(\beta)$ contient un ensemble complet de représentants des classes modulo $\widehat{\mathcal{P}}\widehat{S}$ dans $\widehat{S}$. Par le lemme de Nakayama [Proposition 1.4, page 3,[1]) on aura $\widehat{A}(\beta) = \widehat{S}$ et $\widehat{L} = K_{\mathcal{P}}(\beta)$.
Inversement : Étant donné une racine primitive $p^f - 1$ de l'unité β, on sait que $K_{\mathcal{P}}(\beta)$ est non ramifiée car le discriminant du polynôme $X^n - 1$, avec $n = p^f - 1$ n'est pas divisible par p. Aussi par la considération des racines de l'unité dans les corps finis on en déduit que $[K_{\mathcal{P}}(\beta) : K_{\mathcal{P}}] = f$ □

Corollaire 1.3.2. *Pour chaque entier positive f, il existe une et une seule extension non ramifiée de $K_{\mathcal{P}}$ de dimension f sur $K_{\mathcal{P}}$.*

1.4 Norme Local- Trace et Formule de produit

Soient K un corps de nombres, $L = K(\theta)$ une extension de K et $f(X)$ le polynôme minimal de θ sur K.

Théorème 1.4.1. *Soient $L = K(\theta)$ une extension de K et $f(X)$ le polynôme minimal de θ sur K. Soient $K_{\mathcal{P}}$ le complété de K en $\mathcal{P}$ et $f(X) = f_1(X)\dots f_g(X)$ la factorisation de f sur $K_{\mathcal{P}}$. Alors les premiers de L qui étendent $\mathcal{P}$ correspond un par un aux facteurs $f_i(X)$ de $f(X)$.*
Si $\mathcal{B}_i$ correspond à $f_i(X)$ alors le complété L_i de L en $\mathcal{B}_i$ satisfait $L_i \simeq K_{\mathcal{P}}/(f_i(X))$.

Démonstration. Puisque $f(X)$ est un polynôme séparable, alors les facteurs $f_i(X)$ sont distincts. Par le Théorème de Chinois

$$K_{\mathcal{P}} \otimes_K L \simeq K_{\mathcal{P}} \otimes_K K[X]/(f(X)) \simeq K_{\mathcal{P}}[X]/(f(X)) \simeq K_{\mathcal{P}}[X]/(f_1(X)) \oplus \dots \oplus K_{\mathcal{P}}[X]/(f_g(X)).$$

D'après [Théorème 5.3,Page 114 [1]] les complétés de L en $\mathcal{B}_i$, $1 \le i \le g$, qui étendent $\mathcal{P}$ correspondent un par un aux corps dans la somme directe de $K_{\mathcal{P}} \otimes_K L$ et donc $L_i \simeq L_{\mathcal{B}_i} \simeq K_{\mathcal{P}}[X]/(f_i(X))$. □

Théorème 1.4.2. *On garde les mêmes notations et hypothèses que dans le **Théorème**1.4.1.Alors pour chaque élément $y \in L$ on a :*

1. *Le polynôme caractéristique de y opérant sur L comme $K-$espace vectoriel est égal aux produit des polynômes caractéristiques de y opérant sur $K_{\mathcal{P}}-$espace L_i, $1 \le i \le g$;*

2. $N_{L|K}(y) = \prod_i N_{L_i|K_\mathcal{P}}(y)$ *et* $T_{L|K}(y) = \sum_i T_{L_i|K_\mathcal{P}}(y)$.

Démonstration. Soient $x_1, \ldots, x_n$ une $K-$base de L. Pour $y \in L$ soit r_y la matrice de la transformation $u \mapsto uy$ pour $u \in L$. Donc $1 \otimes x_1, \ldots, 1 \otimes x_n$ est une $K_\mathcal{P}-$base de $K_\mathcal{P} \otimes_K L$ et la multiplication par $1 \otimes y$ donne une transformation linéaire avec une même matrice r_y. On choisit la base de sorte qu'il soit compatible avec $L_1 \oplus \ldots \oplus L_g$. Il s'ensuit que r_y est diagonalisable par bloc et semblable à une matrice de type $diag(r_1, \ldots, r_g)$, où r_i est la matrice de la transformation $u \mapsto uy$ pour $u \in L_i$. On sait

$$P_y(X) = \det(XI_n - r_y) = \prod_i \det(XI_{n_i} - r_i),$$

Qui exprime le polynôme caractéristique de y sur $L|K$ comme produit des polynômes caractéristiques sur $L_i|K_\mathcal{P}$. Par conséquence les assertions du théorème se découlent facilement. □

Lemme 1.4.1. *Soit* $|\ |_\mathcal{P}$ *une valuation sur* K*, l'extension à* L *peut être remplacée par une puissance convenable pour obtenir un ensemble de valuations* $|\ |_i,\ 1 \leq i \leq g$*, tel que pour tout* $y \in L$ *on a :* $\prod_i |y|_i = |N_{L|K}(y)|_\mathcal{P}$.

Démonstration. Soit $\mathcal{P}$ un idéal premier de K et A l'anneau de valuation pour la valuation $|\ |_\mathcal{P}$ dans $\mathcal{P}$. On note aussi par $\mathcal{P}$ l'idéal maximal de A. Soit A' la clôture intégrale de A dans L et supposons que $\mathcal{P}A'$ admet la factorisation suivante

$$\mathcal{P}A' = \mathcal{B}_1^{e_1} \ldots \mathcal{B}_g^{e_g},$$

Si L_i est le complété de L pour la valuation $\mathcal{B}_i-$adique alors on a $[L_i : K_\mathcal{P}] = e_i f_i$.
D'après le [Corollaire 3.4, page 104, [1]] on a l'extension de $|\ |_\mathcal{P}$ à L_i prend la forme

$$|y|_i = |N_{L_i|K_\mathcal{P}}(y)|_\mathcal{P}^{\frac{1}{e_i f_i}}$$

En vertu du **Théorème**1.4.2, on conclu que

$$\prod_i |y|_i^{e_i f_i} = \prod_i |N_{L_i|K_\mathcal{P}}(y)|_\mathcal{P} = |N_{L|K}(y)|_\mathcal{P}.$$

Donc le Lemme est démontré pour les valuations non archimidien.
On le démontre pour le cas archimidien.
Soient $\mathcal{P}_\infty$ un premier infini complexe de K et σ un plongement de K dans $\mathbb{C}$ tel que $|x|_{\mathcal{P}_\infty} = |\sigma(x)|_\mathbb{C}$, où $|\ |_\mathbb{C}$ est le module dans $\mathbb{C}$.

Soient $\sigma_1, \ldots, \sigma_g$ les extensions de σ qui plonge L dans $\mathbb{C}$. Pour $y \in L$ soit $|y|_i = |\sigma_i(y)|_{\mathbb{C}}$ alors

$$\prod_i |y|_i = \prod_i |\sigma_i(y)|_{\mathbb{C}} = |\sigma(N_{L|K}(y))|_{\mathbb{C}} = |N_{L|K}(y)|_{\mathcal{P}_\infty}.$$

Maintenant supposons que $\mathcal{P}_\infty$ un premier infini réel de K et σ un plongement de K dans $\mathbb{R}$ tel que $|y|_{\mathcal{P}_\infty} = |\sigma(y)|_{\mathbb{R}}$, où $|\ |_{\mathbb{R}}$ est la valeur absolue sur $\mathbb{R}$.
Soient $\sigma_1, \ldots, \sigma_a$ tous les extensions de σ qui envoie L sur $\mathbb{R}$ et soit $\sigma_{a+j}, \overline{\sigma_{a+j}}$, $1 \leq j \leq b$ ceux qui plonge L dans $\mathbb{C}$. Soit

$$|y|_i = \begin{cases} |\sigma_i(y)|_{\mathbb{R}} & \text{si } 1 \leq i \leq a \\ |\sigma_i(y)|^2_{\mathbb{C}} & \text{si } a \leq i \leq a+b. \end{cases}$$

Alors on a :

$$\prod_{i=1}^{a+b} |y|_i = \prod_{i=1}^{a} |\sigma_i(y)|_{\mathbb{R}} \prod_{i=a+1}^{a+b} |\sigma_i(y)|^2_{\mathbb{C}} = \prod_{i=1}^{a} |\sigma_i(y)|_{\mathbb{R}} \prod_{i=a+1}^{a+b} |\sigma_i(y)|_{\mathbb{C}} |\overline{\sigma_i}(y)|_{\mathbb{C}} = |\sigma(N_{L|K}(y))|_{\mathbb{C}}.$$

Par conséquence $\prod_{i=1}^{a+b} |y|_i = |N_{L|K}|_{\mathcal{P}}$. □

Proposition 1.4.1. *(Formule de Produit)*
Soient K un corps de nombres et $\mathcal{P}$ un premier de K, il existe une valuation $|\ |_{\mathcal{P}}$ équivalente à la valuation dans $\mathcal{P}$ tel que

$$\forall x \in K^*, \quad \prod_{\mathcal{P} premier} |x|_{\mathcal{P}} = 1,$$

où $\mathcal{P}$ parcourt tous les idéaux premiers de K fini et infini.

Démonstration. Soit $\mathcal{P}$ un premier de $\mathbb{Q}$ et $|\ |_{\mathcal{P}}$ la valuation normalisée sur $\mathbb{Q}$. Soit $\mathcal{B}_1, \ldots, \mathcal{B}_g$ les différents idéaux premiers prolongeant $\mathcal{P}$. Par le **Lemme**1.4.1, il existe une valeur absolue $|\ |_{\mathcal{B}_i}$ équivalente à la valuation dans $\mathcal{B}_i$ tel que

$$\prod_{i=1}^{g} |x|_{\mathcal{B}_i} = |N_{K|\mathbb{Q}}(x)|_{\mathcal{P}}.$$

On écrit $\mathcal{B}_i|\mathcal{P}$ pour indiquer que $\mathcal{B}_i$ prolonge $\mathcal{P}$. On obtient

$$\prod_{\mathcal{P}} \left(\prod_{\mathcal{B}_i|\mathcal{P}} |x|_{\mathcal{B}_i} \right) = \prod_{\mathcal{P}} |N_{K|\mathbb{Q}}(x)|_{\mathcal{P}} = 1.$$

Donc

$$\prod_{\mathcal{B}} |x|_{\mathcal{B}} = \prod_{\mathcal{P},\text{ premier de }\mathbb{Q}} |N_{K|\mathbb{Q}}(x)|_{\mathcal{P}} = 1.$$

D'où le résultat voulu. □

Exemple 1.4.1. Soit $K = \mathbb{Q}(\theta)$, $\theta^3 = 2$, il existe un seul plongement σ_1 de K dans $\mathbb{R}$ tel que $\sigma_1(\theta) = \sqrt[3]{2}$, et deux plongements complexes conjugués σ_2, σ_3 de K dans $\mathbb{C}$ donnés par : $\sigma_2(\theta) = j\sqrt[3]{2}$ et $\sigma_3(\theta) = \overline{j}\sqrt[3]{2}$ avec $j = e^{2i\pi/3}$ et $\overline{j}$ son conjugué. Donc K admet un seul premier infini réel et un premier infini complexe.
Pour la classification des premiers fini de K, il est nécessaire de connaître la factorisation de pA avec p un entier premier et A l'anneau des entiers algébriques de K.

1. $7A = \mathcal{B}_7$ est un idéal premier et la valuation $7-$adique sur $\mathbb{Q}$ admet une unique extension à K. On a $e(\mathcal{B}_7|(7)) = 1$ et $f(\mathcal{B}_7|(7)) = 3$. Il s'ensuit que $[K_{\mathcal{B}_7} : \mathbb{Q}_7] = 3$.

2. Pour $p = 29$ est contenu dans deux premiers $\mathcal{B}_1$ et $\mathcal{B}_2$ dans K admettant des degrés f_1 et f_2 et on a $[K_{\mathcal{B}_1} : \mathbb{Q}_{29}] = 1$ et $[K_{\mathcal{B}_2} : \mathbb{Q}_{29}] = 2$. Ceci donne un exemple tel que $K \neq \mathbb{Q}$ mais $K_{\mathcal{B}} = \mathbb{Q}_{29}$.

3. Les premiers ramifiés sont $p = 2$ et $p = 3$ car le discriminant de K est $-2^2 \times 3^3$, donc Chacun d'eux est contenu dans un unique idéal premier dans A. soient $\mathcal{B}_2$ et $\mathcal{B}_3$ ces deux idéaux respectivement, de degré relative 1 et d'indice de ramification 3 et $[K_{\mathcal{B}_2} : \mathbb{Q}_2] = [K_{\mathcal{B}_3} : \mathbb{Q}_3] = 3$.

Déterminons la valuation $2-$adique sur K :
On a $N_{K_{\mathcal{B}_2}|\mathbb{Q}_2} = N_{K|\mathbb{Q}}$ sur K. Car il existe un seul premier de K prolongeant la $2-$adique valuation. La valuation $K_{\mathcal{B}_2}$ est donnée par :

$$|x|^3 = |N_{K_{\mathcal{B}_2}|\mathbb{Q}_2}(x)|_2,\ x \in K_{\mathcal{B}_2},$$

où $|\ |_2$ est la valuation $2-$adique sur $\mathbb{Q}_2$. On utilise la valuation normalisé $2-$adique $|2|_2 = 1/2$.
Si on se restreint à K on trouve la $2-$adique valuation sur K est donnée par :

$$|x| = |N_{K|\mathbb{Q}}(x)|_2^{1/3}.$$

En particulier :

$$|\theta| = |N_{K|\mathbb{Q}}(\theta)|_2^{1/3} = |2|_2^{1/3} = (\frac{1}{2})^{1/3}.$$

Chapitre 2

Groupe de classes de Rayon

2.1 Généralités

Considérons un corps de nombres K et A(ou A_K) l'anneau des entiers algébriques de K. Si $\mathcal{P}$ un idéal premier fini ou infini de K, On note par $K_{\mathcal{P}}$ le complété de K pour la valuation $\mathcal{P}-$adique.
Le groupe des idéaux $\mathbb{I}_K$ de K est le groupe des idéaux fractionnaires de K. C'est un groupe abelien engendré par les premiers fini. Il existe une application naturelle i de K^* dans $\mathbb{I}_K$ définie par

$$i(\alpha) = (\alpha) = \alpha A.$$

où K^* est le groupe multiplicative des éléments non nuls de K. Le noyau de i est groupe des unités de A. La structure de U_K est donnée par le théorème de Dirichlet. Le conoyau de i noté $\mathbb{I}_K/\mathrm{Im}(i)$ est le groupe de classes de K, noté C_K (ou Cl_K).
Le groupe Cl_K est fini et la suite suivante est exacte.

$$1 \longrightarrow U_K \longrightarrow K^* \longrightarrow \mathbb{I}_K \longrightarrow \mathrm{Cl}(K) \longrightarrow 1$$

2.1.1 Définitions

module

Définition 2.1.1. Un module de K est un produit formel

$$\mathfrak{m} = \prod_{\mathcal{P}} \mathcal{P}^{n(\mathcal{P})}. \tag{2.1}$$

L'idéal $\mathcal{P}$ parcourt tous les idéaux premiers finis ou infinis, pour les quels l'exposant $n(\mathcal{P}) \geq 0$ et $n(\mathcal{P}) > 0$ uniquement pour un nombre fini de $\mathcal{P}$. De plus si $\mathcal{P}$ est premier infini alors

$n(\mathcal{P}) = 0$ ou $n(\mathcal{P}) = 1$.
Si $\mathcal{P}$ est premier infini complexe alors $n(\mathcal{P}) = 0$.

Remarque 5: Un module $\mathfrak{m}$ peut être considéré comme produit $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ où $\mathfrak{m}_0 = \prod_{\mathcal{P}\text{fini}} \mathcal{P}^{n(\mathcal{P})}$ et $\mathfrak{m}_\infty = \prod_{\mathcal{P}\text{réel}} \mathcal{P}^{n(\mathcal{P})}$.
Donc $\mathfrak{m}_0$ est un idéal entier et $\mathfrak{m}_\infty$ est le produit des parties des premiers infinis réels de K.

Congruence multiplicative

- Soit $\mathcal{P}$ un idéal premier réel de K et soit $x \to x_\mathcal{P}$ le plongement de x dans le complété $K_\mathcal{P} = \mathbb{R}$. Pour $\alpha, \beta \in K^*$ on écrit $\alpha \equiv \beta \bmod \mathcal{P}$ pour dire que $\alpha_\mathcal{P}$ et $\beta_\mathcal{P}$ ont le même signe. c'est à dire $(\alpha/\beta)_\mathcal{P} > 0$.

- Si $\mathcal{P}$ est fini. Soit n un entier positive. Dans le localisé $A_\mathcal{P}$ de A les éléments de $1+\mathcal{P}^n A_\mathcal{P}$ sont des unités et forment un sous groupe de $U(A_\mathcal{P})$.
(Noyau de l'homomorphisme $U(A_\mathcal{P}) \longrightarrow U(A_\mathcal{P}/\mathcal{P}^n A_\mathcal{P})$).
Pour deux éléments $\alpha, \beta \in K^*$ on écrit $\alpha \equiv \beta \bmod \mathcal{P}^n$ si $\alpha \in \beta(1 + \mathcal{P}^n A_\mathcal{P})$, c'est à dire $\alpha(1 + \mathcal{P}^n A_\mathcal{P}) = \beta(1 + \mathcal{P}^n A_\mathcal{P})$. En d'autre termes

$$\alpha \equiv \beta \bmod \mathcal{P}^n \Leftrightarrow \alpha/\beta \text{ est une unité de } A_\mathcal{P} \text{ et } v_\mathcal{P}(\alpha/\beta - 1) \geq n.$$

Où $v_\mathcal{P}$ est la valuation exponentielle qui correspond à $\mathcal{P}$.

Définition 2.1.2. Soit $\mathfrak{m}$ un module avec la factorisation Equation2.1.
Pour deux éléments $\alpha, \beta \in K^*$ on écrit $\alpha \equiv \beta \bmod \mathfrak{m}$ si $\alpha \equiv \beta \bmod \mathcal{P}^{n(\mathcal{P})}$ pour tout $\mathcal{P}$ premier de K avec $n(\mathcal{P}) > 0$.

Remarque 6: On vérifie immédiatement que cette congruence est compatible avec le produit mais ne l'est pas avec l'addition. Car K^* n'est pas stable pour l'addition.

Groupe de classes de rayon

Définition 2.1.3. Soit $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ un module, de partie finie $\mathfrak{m}_0$ et de partie infinie $\mathfrak{m}_\infty$. Soit

$$K_\mathfrak{m} = \{a/b \mid \ a,b \in A_K, \text{ et } aA_K, bA_K \ \text{ sont premiers avec } \ \mathfrak{m}_0\}$$
$$K_{\mathfrak{m},1} = \{\alpha \in K_\mathfrak{m} \mid \alpha \equiv 1 \bmod \mathfrak{m}\}.$$

Remarque 7: On a $K_\mathfrak{m}$ et $K_{\mathfrak{m},1}$ sont des sous groupes de K^*. Notons que $K_\mathfrak{m}$ dépend uniquement des premiers finis divisant $\mathfrak{m}$ et pas de leurs exposants. Le groupe $K_{\mathfrak{m},1}$ dépend des premiers finis et infinis divisant $\mathfrak{m}$ et des exposants de ceux qui ont finis.

Soient $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ un module et S un ensemble des premiers finis divisant $\mathfrak{m}_0$.

- On note par $\mathbb{I}_K^S$ (ou $\mathbb{I}^S$) le groupe abelien libre engendré par les idéaux premiers de A_K qui ne sont pas contenus dans S.
- On note par $\mathbb{I}_K^{\mathfrak{m}}$ (ou $\mathbb{I}^{\mathfrak{m}}$) le sous groupe des idéaux engendré par les idéaux premiers ne divisant pas $\mathfrak{m}_0$

$\mathbb{I}^{\mathfrak{m}}$ dépend des premiers finis divisant $\mathfrak{m}$ et pas de leurs exposants.

L'application

$$\begin{array}{rccc} i: & K^* & \to & \mathbb{I}_K \\ & \alpha & \to & i(\alpha) = \alpha A_K \end{array}$$

envoie $K_{\mathfrak{m}}$ et $K_{\mathfrak{m},1}$ dans $\mathbb{I}^{\mathfrak{m}}$.

Définition 2.1.4. Soit $\mathfrak{m}$ un module.

- Le groupe $K_{\mathfrak{m},1}$ s'appelle le `rayon` modulo $\mathfrak{m}$.
- Le quotient $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1})$ s'appel le `groupe de classes de rayon` modulo $\mathfrak{m}$ et les classes dans ce quotient s'appellent les classes de rayon modulo $\mathfrak{m}$.

Exemple 2.1.1. Soit $K = \mathbb{Q}$

1. Soit N un entier naturel. On considère le module $\mathfrak{m} = (N)\mathcal{P}_\infty$. Alors on a :

$$\mathbb{I}^{\mathfrak{m}} = \left\{ \frac{\prod_i \mathcal{P}_i}{\prod_i \mathcal{P}_i'} : \ \mathcal{P}_i, \mathcal{P}_i' \text{ premiers à } N \right\} \simeq \left\{ \left(\frac{a}{b}\right) : \ a,b \in \mathbb{N} \text{ premiers à } N \right\}.$$

   Et $i(K_{\mathfrak{m},1})$ est le sous groupe engendré par $\frac{(a)}{(b)}$ avec $a \equiv b \bmod N$ et $a/b > 0$. Ce qui équivalent à $\alpha \equiv 1 \bmod N$, avec $\alpha \in \mathbb{Q}^+$. Donc $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1}) = (\mathbb{Z}/N\mathbb{Z})^\times$.

2. soit $\mathfrak{m} = (N)$. Alors $i(K_{\mathfrak{m},1})$ est le sous groupe engendré par (a) avec $a \equiv 1 \bmod N$ et $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1}) = (\mathbb{Z}/N\mathbb{Z})^\times / \{-1,1\}$

Exemple 2.1.2.

1. Soit $K = \mathbb{Q}(i)$ and $\mathfrak{m} = (3)$. Alors $\mathbb{I}^{\mathfrak{m}}$ l'ensemble des idéaux fractionnaires premiers à 3 et $i(K_{\mathfrak{m},1})$ ceux engendrés par les éléments α tel que $\alpha \equiv 1 \bmod 3$. Ainsi
$$\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1}) \simeq (\mathbb{Z}[i]/(3))^\times/\{\pm 1, \pm i\} \simeq C_2.$$
2. Soit $K = \mathbb{Q}(\sqrt{-5})$ et $\mathfrak{m} = (3) = \mathcal{P}_3\mathcal{P}_3'$. Puisque $\mathcal{P}_2$ est un idéal non principal au dessus de 2 on aura $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1}) \simeq C_2 \times C_2 =< [\mathcal{P}_2], [\sqrt{-5}] >$.

2.1.2 Théorème d'Approximation

Théorème 2.1.1. *Soient* $|\ |_1,\ldots,|\ |_n$ *des valuations deux à deux non équivalentes sur* K *et* $\beta_1,\ldots,\beta_n$, n *éléments de* K. *Alors :*
Pour tout réel positive ϵ *; il existe* $\alpha \in K$ *tel que* $|\alpha-\beta_i|_i<\epsilon,\ \forall i=1,\ldots,n$.

Démonstration. En premiers temps, on montre qu'il existe des éléments $y_1,\ldots,y_n$ dans K tel que $|y_i|_i>1$ et $|y_i|_j<1$ pour tout $i\neq j$.
Pour cela nous utilisons l'induction sur n :
Pour $n=2$, la définition de l'équivalence implique qu'il existe des éléments w et z tel que : $|w|_1\geq 1$ et $|w|_2<1$, aussi $|z|_1<1$ et $|z|_2\geq 1$.
Soit $y=w/z$, donc $|y|_1>1$ et $|y|_2<1$.
On suppose qu'il existe y tel que $|y|_1>1$ et $|y|_j<1$, $j=2,\ldots,n-1$. Par le cas "$n=2$" (deux valeurs absolues), il existe t tel que $|t|_1>1$ et $|t|_n<1$. Soit y_1 construit comme suit

$$y_1=\begin{cases} y & \text{si}\quad |y|_n<1\\ y^r t & \text{si}\quad |y|_n=1\\ \frac{y^r t}{1+y^r} & \text{si}\quad |y|_n>1\end{cases}$$

où r un entier que l'on déterminera.
Pour le deuxième cas on a $|y_1|_j=|y|_j^r|t|_j$, $2\leq j\leq n$, donc $|y_1|_j<1$ lorsque r est assez grand, car $|y|_j<1$, $j=2,\ldots,n-1$ et pour $j=n$ on a $|t|_n<1$.
Pour le dernier cas on a la même conclusion car $\frac{|y^r|_j}{|1+y^r|_j}<\frac{1}{|y^{-r}|_j-1}$, et a une limite nulle quand r tend vers $+\infty$.
Dans tous les cas on a construit un élément y_1 de sorte que $|y_1|_1>1$ et $|y_1|_j<1$, $2\leq j\leq n$.
Par symétrie on obtient des éléments $y_1,y_2,\ldots,y_n$ qui vérifient $|y_i|_i>1$ et $|y_i|_j<1$, $\forall j\neq i$.
Pour finir la preuve considérons $\alpha=\sum_{i=1}^{n}\frac{y_i^s}{1+y_i^s}\beta_i$, où s est un entier que l'on déterminera. L'inégalité triangulaire entraîne que

$$|\alpha-\beta_i|_i\leq|\frac{\beta_i}{1+y_i^s}|_i+\sum_{j\neq i}|\frac{y_j^s\beta_j}{1+y_j^s}|_i.$$

Pour s assez grand l'expression doit être inférieure à ϵ. □

Remarque 8:

- Soit $\mathcal{P}_\infty$ un idéal premier infini réel de K.
  Pour $\alpha\beta\neq 0$ l'assertion $|\alpha-\beta|_{\mathcal{P}}<\epsilon$ pour ϵ assez petit, implique que $\alpha_{\mathcal{P}}$ et $\beta_{\mathcal{P}}$ ont le

même signe. Donc $\alpha \equiv \beta \bmod \mathcal{P}$.

- Si $\mathcal{P}$ est un premier fini. la valuation $\mathcal{P}-$adique, v qui satisfait $|\alpha|_{\mathcal{P}} = c^{v(\alpha)}$, pour $0 < c < 1$ et $v(\alpha)$ est la puissance de $\mathcal{P}$ qui apparaît dans la factorisation de $i(\alpha)$. Soit α et β deux éléments de K^* tel que $|\alpha - \beta|_{\mathcal{P}} < \epsilon$ alors $|\alpha/\beta - 1|_{\mathcal{P}} < \epsilon/|\beta|_{\mathcal{P}} = \epsilon'$. Lorsque ϵ' est assez petit, $\epsilon' < c^n$, donc $v(\alpha/\beta - 1) > n$, il s'ensuit que $\alpha/\beta \in 1 + \mathcal{P}^n A_{\mathcal{P}}$ et donc $\alpha \equiv \beta \bmod \mathcal{P}$.

Proposition 2.1.1. *Soient* $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ *des modules premiers entre deux à deux et* $\mathfrak{m} = \mathfrak{m}_1 \times \ldots \times \mathfrak{m}_n$ *leur produit. L'application*

$$\begin{array}{ccc} K_{\mathfrak{m}} & \to & K_{\mathfrak{m}_1}/K_{\mathfrak{m}_1,1} \times \ldots \times K_{\mathfrak{m}_1}/K_{\mathfrak{m}_n,1} \\ \alpha & \mapsto & (\alpha K_{\mathfrak{m}_1,1}, \ldots, \alpha K_{\mathfrak{m}_n,1}) \end{array}$$

induit un isomorphisme

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \simeq K_{\mathfrak{m}_1}/K_{\mathfrak{m}_1,1} \times \ldots \times K_{\mathfrak{m}_n}/K_{\mathfrak{m}_n,1}$$

Démonstration. Soit ϕ l'application définie par

$$\begin{array}{rccc} \phi: & K_{\mathfrak{m}}/K_{\mathfrak{m},1} & \to & K_{\mathfrak{m}_1}/K_{\mathfrak{m}_1,1} \times \ldots \times K_{\mathfrak{m}_n}/K_{\mathfrak{m}_n,1} \\ & \alpha K_{\mathfrak{m},1} & \mapsto & (\alpha K_{\mathfrak{m}_1,1}, \ldots, \alpha K_{\mathfrak{m}_n,1}). \end{array}$$

Le noyau de ϕ est l'ensemble des classes $\alpha K_{\mathfrak{m},1}$ tel que $\alpha \in \bigcap_{i=1}^{n} K_{\mathfrak{m}_i,1}$, donc $\alpha \in K_{\mathfrak{m},1}$. D'où l'injection.
Montrons qu'elle est surjective. Soit $\beta_i \in K_{\mathfrak{m}_i}$, il existe $\alpha \in K$ tel que $|\alpha - \beta_i|_{\mathcal{P}} < \epsilon$ pour tout $\mathcal{P}$ divisant $\mathfrak{m}$ et ϵ assez petit. Ceci signifie que $\alpha/\beta_i \equiv 1 \bmod \mathfrak{m}_i$ pour tout $1 \leq i \leq n$. Ce qui implique que pour tout i, $\alpha/\beta_i \in K_{\mathfrak{m}_i,1}$ et $\alpha K_{\mathfrak{m},1} = \beta_i K_{\mathfrak{m}_i,1}$, d'où la surjection. □

Corollaire 2.1.1. *Pour tout module* $\mathfrak{m}$*, le groupe* $K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ *est fini.*

Démonstration. D'après La **Proposition**2.1.1, on remarque qu'il suffit de prouver cela pour le cas $\mathfrak{m}$ est divisible uniquement par un premier de K.
Supposons que $\mathfrak{m}$ est réel, alors $K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ est le groupe quotient K^* modulo le sous groupe des éléments positifs en $\mathfrak{m}$. Ce groupe est d'ordre 2.
Maintenant supposons que $\mathfrak{m} = \mathcal{P}^n$ avec $\mathcal{P}$ un premier de A_K et n un entier positif. Dans ce cas $K_{\mathfrak{m}}$ est le groupe des unités locaux de $A_{\mathcal{P}}$ et $K_{\mathfrak{m},1}$ est le groupe $1 + \mathcal{P}A_{\mathcal{P}}$. Il s'ensuit que $K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ est le groupe des unités de l'anneau $A_{\mathcal{P}}/\mathcal{P}^n$. Puisque il est fini de cardinal $\mathcal{N}_{K|Q}(\mathcal{P}^n)$, donc son groupe des unités doit être fini. □

Proposition 2.1.2. *Soit $\mathfrak{m}$ un module. Alors toute classe de $K_\mathfrak{m}$ modulo $K_{\mathfrak{m},1}$ contient un élément relativement premier à un idéal donné.*

Démonstration. Etant donné un idéal $\mathcal{U} = \prod_i \mathcal{Q}_i^{a_i}$ et soit $\beta K_{\mathfrak{m},1}$ une classe modulo $K_{\mathfrak{m},1}$, avec $\beta \in K_\mathfrak{m}$.
Par la **Proposition**2.1.1 appliquée à $\mathfrak{m}\prod \mathcal{Q}_i^{a_i}$, il existe un élément γ tel que

$$\gamma \equiv \beta \bmod \mathfrak{m},\ \gamma \equiv 1 \bmod \mathcal{Q}_j^{a_j}.$$

Où $\mathcal{Q}_j$ parcourt les facteurs premiers de $\mathcal{U}$ ne divisant pas $\mathfrak{m}$. Donc β et γ sont dans la même classe modulo $K_{\mathfrak{m},1}$ et γ est premier à $\mathcal{U}$. □

2.2 Propriétés du groupe de Classes de Rayon

Proposition 2.2.1. *Soit S un ensemble fini des idéaux premiers. Alors $C_K = \mathbb{I}_K/i(K^*)$ est isomorphe à $\mathbb{I}^S/\mathbb{I}^S \cap i(K^*)$.*

Démonstration. L'inclusion $\mathbb{I}^S \longrightarrow \mathbb{I}_K$ induit une inclusion de $\mathbb{I}^S/\mathbb{I}^S \cap i(K^*)$ vers $C_K = \mathbb{I}_K/i(K^*)$.
Soit $\mathfrak{a}$ la classe d'un idéal $\mathcal{A}$. Montrons qu'il contient un représentant qui n'est pas divisible par aucun premier dans S. Pour un idéal $\mathcal{B}$ dans $\mathbb{I}_K$, écrivons $\mathcal{B} = \mathcal{B}_1\mathcal{B}_2$ où $\mathcal{B}_1$ n'est pas divisible par aucun premier dans S et $\mathcal{B}_2 = \prod_{\mathcal{P}\in S} \mathcal{P}^{n(\mathcal{P})}$.
Soit $\pi_\mathcal{P}$ l'élément de K^* qui engendre $\mathcal{P}$ dans $A_\mathcal{P}$ (localisé de A en $\mathcal{P}$), et qui satisfait $\pi_\mathcal{P} \equiv 1 \bmod \mathcal{Q}$ pour tout $\mathcal{Q} \in S$, $\mathcal{Q} \neq \mathcal{P}$. Un tel élément existe par le théorème de Chinois. Soit $\alpha = \prod_{\mathcal{P}\in S} (\pi_\mathcal{P})^{n(\mathcal{P})}$. l'idéal $\mathcal{P}^{n(\mathcal{P})}$ divise $i(\alpha)$. Donc $\mathcal{B}\alpha^{-1}$ n'est pas divisible par aucun premier de S et appartenant à la même classe de $\mathcal{B}$. Il s'ensuit que chaque classe dans C_K a un représentant dans $\mathbb{I}^S$. □

Corollaire 2.2.1. *Soit $\mathfrak{m}$ un module quelconque, le groupe de classes de rayon $\mathbb{I}^\mathfrak{m}/i(K_{\mathfrak{m},1})$ est un groupe fini.*

Démonstration. On a $\mathbb{I}^\mathfrak{m} \cap i(K^*)$ est l'ensemble des idéaux principaux premiers à la partie réelle $\mathfrak{m}_0$ de $\mathfrak{m}$. Donc $\mathbb{I}^\mathfrak{m} \cap i(K^*) = i(K_\mathfrak{m})$. Alors on aura :

$$[\mathbb{I}^\mathfrak{m} : i(K_{\mathfrak{m},1})] = [\mathbb{I}^\mathfrak{m} : i(K_\mathfrak{m})][i(K_\mathfrak{m}) : i(K_{\mathfrak{m},1})] \tag{2.2}$$

De la **Proposition**2.2.1, on déduit que le premier facteur est le nombre de classes $h(K)$ et le deuxième facteur est un diviseur de $[K_\mathfrak{m} : K_{\mathfrak{m},1}]$ qui est fini. □

L'ordre du groupe de classes de rayon $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1})$ est noté $h_{\mathfrak{m}}$ et s'appel le nombre de classes de rayon.

Corollaire 2.2.2. *Soient K un corps de nombre et $\mathfrak{m}$ un module de K. Alors le nombre de classes h_K de K divise le nombre de classes de rayon $h_{\mathfrak{m}}$. Avec l'égalité si $\mathfrak{m} = (1)$.*

Démonstration. Le résultat se découle facilement de l'Equation2.2 et du fait que si $\mathfrak{m} = (1)$ le groupe de classe de rayon est C_K. □

Proposition 2.2.2. *Soit $\mathfrak{m}$ un module alors chaque classe de $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1})$ contient un idéal entier.*

Démonstration. Le groupe $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1})$ est fini. Donc pour chaque idéal $\mathcal{P}$ de $\mathbb{I}^{\mathfrak{m}}$ il existe $k \in \mathbb{N}$ tel que $\mathcal{P}^k \in i(K_{\mathfrak{m},1})$. Soit $\mathcal{U}$ un élément d'une classe $\mathbf{k}$, donc $\mathcal{U} = \mathcal{U}_1\mathcal{U}_2^{-1}$ avec $\mathcal{U}_1$ et $\mathcal{U}_2$ deux idéaux entiers de $\mathbb{I}^{\mathfrak{m}}$. Soit $r > 1$ tel que $\mathcal{U}_2^r \in i(K_{\mathfrak{m},1})$, il s'ensuit que $\mathcal{U}\mathcal{U}_2^r$ est un idéal de entier tel que $\mathbf{k}\mathcal{U}_2^r = \mathbf{k}$. □

Régulateur d'un module $\mathfrak{m}$

Le groupe U_K des unités de A est un sous groupe de K_m. Comme $K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ est fini alors $U_K/(U_K \cap K_{\mathfrak{m},1})$ est fini.
Nous considérons l'application l définie sur U_K par $l(a) = (l_1(a), \ldots, l_{r+s}(a))$, où

$$l_i(a) = \begin{cases} \ln|\sigma_i(a)| & \text{si } 1 \leq i \leq r \\ 2\ln|\sigma_i(a)| & \text{si } r < i \leq r+s. \end{cases}$$

Avec σ_i, $1 \leq i \leq r$ sont les plongements réels de K et $\sigma_i, \overline{\sigma_i}$ avec $r < i \leq r+s$ les plongements complexes de K.
On remarque que l envoie U_K sur une lattice de $\mathbb{R}^{r+s}$ de dimension $r+s-1$. Il s'ensuit que $l(U_K \cap K_{\mathfrak{m},1})$ admet un indice fini dans $l(U_K)$ et il est de même une lattice de dimension $r+s-1$.
soient $\{w_1, \ldots, w_{r+s-1}\}$ les éléments de $U_K \cap K_{\mathfrak{m},1}$ dont les images par l donnent une $\mathbb{Z}-$base de $l(U_K \cap K_{\mathfrak{m},1})$.
Comme la somme des coordonnées de chaque $W_i = l(w_i)$ est égale à zéro, on en déduit que la famille $\{W, W_1, \ldots, W_{r+s-1}\}$ est une famille libre. Et forme une $\mathbb{Z}$ base de $\mathbb{R}^{r+s}$, où $W = (1, \ldots, 1, 2 \ldots, 2)$ avec r un et s deux.

Définition 2.2.1. On garde les mêmes les notations, le régulateur du module $\mathfrak{m}$ est donné par : $\mathrm{reg}(m) = \frac{1}{r+2s} \det(W, W_1, \ldots, W_{r+s})$.

Proposition 2.2.3. *Soient K un corps de nombre, $\mathfrak{m}$ un module de K et $\{\epsilon_1, \ldots, \epsilon_{r+s-1}\}$ une base de $U_K \cap K_{\mathfrak{m},1}$. Alors le régulateur de $\mathfrak{m}$ est donnée par :*
$\mathrm{reg}(m) = \det\left(\delta_i\left(\sigma_i(\epsilon_j)\right)_{1\leq i,j\leq r+s-1}\right)$, *où $\delta_i = 1$ si σ_i est réel et $\delta_i = 2$ si σ_i est complexe.*

Démonstration. La démonstration se découle facilement du fait que la somme des coordonnées des vecteurs W_i est zéro et le fait que le déterminant reste inchangé si on ajoute à une ligne ou à une colonne une combinaison des linéaire des autres. □

Remarque 9: Si $\mathfrak{m} = (1)$ le régulateur de $\mathfrak{m}$ est le régulateur de K.

Théorème 2.2.1. *Soient K un corps de nombre, $\mathfrak{m}$ un module de K. et $\mathbf{k}$ une classe dans $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1})$. Alors :*
Le nombre des idéaux entier dans $\mathbf{k}$ de norme au plus n, avec $n \in \mathbb{N}^*$, noté $S(n,\mathbf{k})$ vérifié :

$$\lim_{n\to\infty} \frac{S(n,\mathbf{k})}{n} = \frac{2^{r+s} reg(\mathfrak{m})\pi^s}{\omega_{\mathfrak{m}}\mathcal{N}(\mathfrak{m})\sqrt{|\Delta_K|}}.$$

où

- $reg(\mathfrak{m})$ *le régulateur de* $\mathfrak{m}$,
- $r + 2s = d = [K : \mathbb{Q}]$,
- r *le nombre des premiers infinis réels,*
- s *le nombre des premiers infinis complexes,*
- $\omega_{\mathfrak{m}}$ *le nombre des racines de l'unité dans,* $U_K \cap K_{\mathfrak{m},1}$,
- Δ_K *le discriminant de* A_K *sur* $\mathbb{Z}$.

Démonstration. Pour la démonstration (Voir [1], page 146-152 et page 73-77, (Cours unités des corps de nombres)) □

Remarque 10: La limite du **Théorème**2.2.1 ne dépend pas de la classe de $\mathbf{k}$, mais elle dépend de K et de $\mathfrak{m}$.

Deuxième partie

Fonction zeta des corps de nombres ; $L-$fonction et Applications

Chapitre 3

Fonction Zeta et $L-$Fonction

3.1 Généralités

On note par $D(b,\delta,\epsilon) = \{s \in \mathbb{C} \,|\, Re(s) \geq b+\delta, \,|\, |arg(s-b)| \leq \pi/2 - \epsilon\}$, où δ et ϵ deux nombres réels positifs et b un nombre réel.

3.1.1 Séries de Dirichlet

Définition 3.1.1. La fonction définie sur $\mathbb{C}$ par :

$$f(s) = \sum_{n\geq 1} \frac{a(n)}{n^s} \tag{3.1}$$

où $a(n)$ des nombres complexes et $s = \sigma + it$ un nombre complexe. Lorsque la série $\sum\limits_{n\geq 1} \frac{a(n)}{n^s}$ converge, elle s'appelle la série de Dirichlet. Si $a(n) = 1,\ \forall n \in \mathbb{N}$, la fonction f est la fonction ζ de Riemann donnée par $\zeta(s) = \sum\limits_{n\geq 1} \frac{1}{n^s}$.

Proposition 3.1.1. *Soit $f(s)$ la série de Dirichlet et soit $S(x) = \sum\limits_{n\leq x} a(n)$. On suppose qu'il existe deux constantes a et b tel que $|S(x)| \leq ax^b$, $\forall x \geq r$ $(r > 0)$. Alors on a les assertions suivantes*

1. *La série $f(s)$ est uniformément convergente dans $D(b,\delta,\epsilon)$ avec ϵ et δ des nombres positifs.*
2. *La fonction $f(s)$ est analytique dans le demi plan $Re(s) > b$*

Démonstration. 1. Notons que $a(n) = S(n) - S(n-1)$, si $v \geq u+1$ alors on a :

$$\begin{aligned}
\left|\sum_{n=u}^{v} \tfrac{a(n)}{n^s}\right| &= \left|\sum_{n=u}^{v} \tfrac{S(n)}{n^s} - \sum_{n=u-1}^{v-1} \tfrac{S(n)}{(n+1)^s}\right| \\
&= \left|\tfrac{S(v)}{v^s} - \tfrac{S(u-1)}{u^s} + \sum_{n=u}^{v-1} S(n)\left(\tfrac{1}{n^s} - \tfrac{1}{(n+s)^s}\right)\right| \\
&\leq \left|\tfrac{S(v)}{v^s}\right| + \left|\tfrac{S(u-1)}{u^s}\right| + \sum_{n=u}^{v-1} |S(n)| \left|\tfrac{1}{n^s} - \tfrac{1}{(n+s)^s}\right|
\end{aligned}$$

Or $n > 0$, $|n^s| = |n^{\sigma+it}| = n^\sigma$ et $\frac{1}{n^s} - \frac{1}{(n+1)^s} = s\int_n^{n+1} \frac{dt}{t^{s+1}}$. Donc

$$\left|\sum_{n=u}^{v} \frac{a(n)}{n^s}\right| \leq \frac{a}{v^{\sigma-b}} + \frac{a}{v^{\sigma-b}} + \sum_{u}^{v-1} |s|(an^b) \left|\int_n^{n+1} \frac{dt}{t^{s+1}}\right|$$

Comme

$$\sum_{u}^{v-1} |s|(an^b) \left|\int_n^{n+1} \frac{dt}{t^{s+1}}\right| \leq |s|a\int_u^\infty \frac{t^b dt}{|t^{s+1}|} \leq |s|a\int_u^\infty \frac{dt}{t^{\sigma+1-b}} = \frac{a|s|}{(\sigma-b)u^{\sigma-b}},$$

et $v > u$ il vient que :

$$\left|\sum_{n=u}^{v} \frac{a(n)}{n^s}\right| \leq \frac{2a}{u^{\sigma-b}} + \frac{a|s|}{(\sigma-b)u^{\sigma-b}}.$$

Soit $\theta = \arg(s-b)$, alors

$$\frac{s}{u^{\sigma-b}} \leq \frac{|s-b|+b}{u^{\sigma-b}} \leq \frac{1}{cos(\theta)} + \frac{b}{\delta}.$$

Le nombre $\frac{b}{\delta}$ est constant et la relation $|\theta| \leq \pi/2 - \epsilon$ signifie qu'il existe une constante M tel que $\frac{1}{\cos(\theta)} < M$, $\forall s \in D(b,\delta,\epsilon)$. Donc pour tout ϵ, il existe N tel que $\forall u \geq N$:

$$\frac{2a}{u^{\sigma-b}} + \frac{a|s|}{(\sigma-b)u^{\sigma-b}} \leq \frac{2a + a(M + b/\delta)}{u^{\sigma-b}} < \epsilon. \text{ (tend vers 0 lorsque } u \to \infty)$$

Ce implique que la convergence est uniforme dans $D(b,\delta,\epsilon)$.

2. On a chaque point dans le demi plan $Re(s) > b$ appartient à $D(b,\delta,\epsilon)$ pour b, δ et ϵ bien choisies. Or dans $D(b,\delta,\epsilon)$ la série est uniformément convergente à une fonction analytique, et donc il représente une fonction analytique sur $Re(s) > b$.

□

Proposition 3.1.2. *Soit* $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$ *la fonction* ζ *de Riemann. Alors*

$$\lim_{s\to 1}(s-1)\zeta(s) = 1$$

Démonstration. On montre que la fonction $s \to (s-1)\zeta(s)$ est une fonction analytique dans $D(1,1/2) = \{s \mid |s-1| < 1/2\}$ et on passe à la limite suivant la direction l'axe réel à droite de $s = 1$.

Considérons la fonction

$$\zeta_2(s) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^s}$$

La somme des n premiers termes est 0 ou 1. Par la **Proposition**3.1.1, on en déduit que la fonction $\zeta_2(s)$ est uniformément convergente dans $D(0,\delta,\epsilon)$. En particulier elle est analytique sur le disque $|s-1| < 1/2$.
Aussi remarquons que :

$$\zeta_2(s) + \frac{2}{2^s}\zeta(s) = \zeta(s).$$

Donc $\zeta(s) = \left(1 - \frac{1}{2^{s-1}}\right)^{-1} \zeta_2(s)$ dans l'intersection des régions de convergences.
La fonction $\left(1 - \frac{1}{2^{s-1}}\right)^{-1} \zeta_2(s)$ est le quotient de la fonction analytique $\zeta_2(s)$ et la fonction $\left(1 - \frac{1}{2^{s-1}}\right)$. Cette dernière (qui est dans le dénominateur) s'annule uniquement lorsque $2^{s-1} = 1$ c'est à dire lorsque s prend les valeurs $s = 1 + \frac{2ik\pi}{\ln 2}$ où k un entier.
Le pôle réel de $\zeta(s)$ peut être réalisé uniquement lorsque $s = 1$. On vérifie que les autres points ne sont pas des pôles.
Considérons la fonction

$$\zeta_3(s) = \frac{1}{1^s} + \frac{1}{2^s} - \frac{2}{3^s} + \ldots + \frac{1}{3k+1^s} + \frac{1}{3k+2^s} - \frac{2}{3k+3^s} + \ldots$$

La somme des coefficients de cette fonction est égale à 0 ou 1 ou 2 et donc $\zeta_3(s)$ est uniformément convergente dans $D(0,\delta,\epsilon)$. Comme ci-dessus on trouve dans l'intersection des domaines de convergences que $\zeta(s) = \left(1 - \frac{1}{3^{s-1}}\right)^{-1} \zeta_3(s)$.
Les pôles possibles de $\zeta(s)$ sont les points $s = 1 + \frac{2im\pi}{\ln 3}$.
Si un point s est un pôle de ζ alors $s = 1 + \frac{2im\pi}{\ln 3}$ et $s = 1 + \frac{2ik\pi}{\ln 2}$ et donc $2^m = 3^k$. Puisque m et k des entiers, il s'ensuit que $m = k = 0$. Donc ζ admet un unique pôle en $s = 1$.
Montrons que le pôle $s = 1$ est simple.
Soit s un nombre réel tel que $s > 1$ alors on a :

$$\zeta(s) \leq 1 + \int_1^{+\infty} \frac{dx}{x^s} = 1 + \frac{1}{s-1} \text{ et } \zeta(s) \geq \int_1^{+\infty} \frac{dx}{x^s}.$$

Donc $1 \leq (s-1)\zeta(s) \leq s$ pour tout $s > 1$. Par passage à la limite on trouve le résultat. □

Corollaire 3.1.1. *On garde les notations et hypothèses de la* ***Proposition****3.1.1. Alors :*
Si $\lim\limits_{x\to\infty} \frac{S(x)}{x} = a_0$ *alors* $\lim\limits_{s\to 1}(s-1)f(s) = a_0,\ s \in D(1,0,\epsilon)$

Démonstration. On suppose que $\lim\limits_{x\to\infty} \frac{S(x)}{x} = a_0$. Alors $S(x) = a_0 x + e(x)x$ où $e(x) \to 0$ lorsque $x \to +\infty$. Nécessairement $e(x)$ est une fonction bornée, donc il existe une constante a_2 tel que $|S(x)| \leq a_2 x$. Par la **Proposition**3.1.1, la fonction $f(s)$ est uniformément convergente dans

$D(1,\delta,\epsilon)$ pour $(\delta, \epsilon > 0)$.
La démonstration consiste à montrer que $(s-1)f(s)$ à la même limite lorsque $s = 1$ que $a_0(s-1)\zeta(s)$, où $\zeta(s)$ est la fonction ζ de Riemann.
On a :

$$\begin{aligned} |f(s) - a_0\zeta(s)| &= \left|\sum_{n\geq 1} \tfrac{a(n)-a_0}{n^s}\right| = \left|\sum_{n\geq 1}(S(n)-na_0)(\tfrac{1}{n^s} - \tfrac{1}{n^{s+1}})\right| \\ &\leq \left|\sum_{n\geq 1} ne(n)s\int_n^{n+1}\tfrac{dt}{t^{s+1}}\right| \leq n|e(n)||s|\int_n^{n+1}\tfrac{dt}{t^{\sigma+1}}. \end{aligned}$$

Soit $\epsilon_0 > 0$ et N un entier assez grand tel que $n > N,\ |e(n)| < \epsilon_0$. Soit M une borne de $e(n)$ pour tout $n \in \mathbb{N}$. Alors, comme $n\int_n^{n+1}\frac{dt}{t^{\sigma+1}} \leq \int_n^{n+1}\frac{t}{t^{\sigma+1}}dt$, on trouve

$$|s-1||f(s) - a_0\zeta(s)| \leq |s(s-1)|M\int_1^N \frac{dt}{t^\sigma} + \left|s(s-1)\epsilon_0\int_N^{+\infty}\frac{dt}{t^\sigma}\right|.$$

La limite lorsque $s \to 1$ du premier terme dépend de l'intégrale $\int_1^N \frac{dt}{t^\sigma}$. Cet intégrale existe lorsque $s \in D(1,0,\epsilon)$ et donc la limite est zéro.
La limite du deuxième terme dépend de l'autre intégrale, elle est égale à $\frac{|s(s-1)|\epsilon_0}{\sigma-1} \times \frac{1}{N^{\sigma-1}}$. Si $s \in D(1,0,\epsilon)$, alors $\frac{s-1}{\sigma-1} \leq \pi/2 - \epsilon = A_0$. Donc lorsque s est au voisinage de 1 et dans $D(1,0,\epsilon)$ on aura

$$|s-1||f(s) - a_0\zeta(s)| < \epsilon_0 A_0.$$

Puisque ϵ_0 est choisi arbitraire on en déduit que

$$\lim_{s\to 1}((s-1)f(s) - a_0(s-1)\zeta(s)) = 0.$$

Le résultat se découle du fait que $\lim_{s\to 1}(s-1)\zeta(s) = 1$ (**Proposition3.1.2**). □

3.1.2 Du Produits infinis aux séries

Soit *Logz* une branche logarithmique ayant la partie imaginaire dans $[-\pi/2,\pi/2]$. On a :

$$Logz = ln|z| + i\arg z, \text{ avec } -\pi/2 \leq argz \leq \pi/2.$$

Donc si z est réel *Logz* est réelle. La fonction *Log* se développe en série entière au voisinage de 1 comme suit

$$-Log(1-z) = z + \frac{z^2}{2} + \ldots,\ |z| < 1$$

Proposition 3.1.3. *Soit (u_i) une suite de nombre réel tel que $\forall i, u_i \geq 2$. Supposons que la*

fonction $g(s)=\prod_j \left(1-u_j^{-s}\right)^{-1}$ *converge uniformément dans chaque région* $D(1,\delta,\epsilon)$ *pour* $\delta>0$ *et* $\epsilon>0$. *Alors*

$$Log(g(s))=\sum_j u_j^{-s}+h(s).$$

Où $h(s)$ *est une fonction bornée au voisinage de* 1.

Démonstration. La convergence uniforme permet de faire les manipulations suivantes

$$\begin{aligned} Log(g(s)) &= -\sum_j Log(1-u_j^{-s})=\sum_j \sum_{m=1}^{+\infty} \tfrac{1}{mu_j^{sm}} \\ &= \sum_j \tfrac{1}{u_j^s}+\sum_j \sum_{m=2}^{+\infty} \tfrac{1}{mu_j^{sm}}=\sum_j \tfrac{1}{u_j^s}+h(s). \end{aligned}$$

où $h(s)=\sum_j \sum_{m=2}^{+\infty} \frac{1}{mu_j^{sm}}$.

Soit $\sigma=Re(s)$, alors on obtient après majoration que $|h(s)|\leq \sum_j \sum_{m=2}^{+\infty} \frac{1}{mu_j^{m\sigma}}\cdot$ Or on a $\sum_{m=2}^{+\infty} \frac{1}{mu_j^{m\sigma}} \leq \sum_{m=2}^{+\infty} \frac{1}{2u_j^{m\sigma}}=\frac{1}{2}\left(\frac{1}{1-u_j^{-\sigma}}-u_j^{-\sigma}-1\right)$, ainsi $\sum_{m=2}^{+\infty} \frac{1}{mu_j^{m\sigma}} \leq \frac{1}{u_j^{2\sigma}}$. Donc $|h(s)|\leq \sum_j \frac{1}{u_j^{1\sigma}}\cdot$
La convergence de $f(2\sigma)$ pour $2\sigma>1+\delta$ implique que $h(s)$ est bornée en $\sigma=1$ et en $s=1$. En particulier dans le disque $|s-1|<1/2$. □

Proposition 3.1.4. *(Formule d'Euler)*
Pour tout $s\in\mathbb{C}$ *tel que* $Re(s)>1$ *on a :*

$$\zeta(s)=\prod_{p\ premier}\left(1-\frac{1}{p^s}\right)^{-1}$$

Démonstration. Soit $s=\sigma+it$, avec $\sigma>1$. Pour tout premier p on a $\left(1-\frac{1}{p^s}\right)^{-1}=\sum_{k=0}^{+\infty}\frac{1}{p^{ks}}$. En prenant le produit pour p premier et $p\leq N$ avec (N>2) on obtient :

$$\begin{aligned} \prod_{p\leq N}\left(1-\tfrac{1}{p^s}\right)^{-1} &= \prod_{p\leq N}\sum_{k=0}^{+\infty}\tfrac{1}{p^{ks}} \\ &= \sum_{k_1,\ldots,k_n\geq 0}\tfrac{1}{\left(p_1^{k_1}\ldots p_n^{k_n}\right)^s}. \end{aligned}$$

Où $p_1<\ldots<p_n$ désignent les nombres premiers inférieurs à N.
Donc $\prod_{p\leq N}\left(1-\frac{1}{p^s}\right)^{-1}=\sum_{g(n)\leq N}\frac{1}{n^s}$, où $g(n)$ est le plus grand nombre premier divisant n. Or

comme $\{1,\ldots,N\} \subset \{n \in \mathbb{N}^*, | \, g(n) \leq N\}$, alors

$$\left|\zeta(s) - \prod_{p \leq N} \left(1 - \frac{1}{p^s}\right)^{-1}\right| \leq \sum_{n \geq N} \frac{1}{n^\sigma}.$$

En faisant tendre N vers l'infini on obtient le résultat. □

3.1.3 Prolongement de la fonction ζ de Riemman

Prolongement de ζ au demi plan $Re(s) > 0$

Pour $Re(s) > 1$, on pose $f_1(s) = \zeta(s) - \frac{1}{s-1}$. Il vient que $f_1(s) = \sum\limits_{n \geq 1} \frac{1}{n^s} - \int_1^{+\infty} \frac{1}{x^s} dx = \sum\limits_{n \geq 1} \int_n^{n+1} (\frac{1}{n^s} - \frac{1}{x^s}) dx$.

Posons pour tout $n \in \mathbb{N}^* : \phi_n(s) = \int_n^{n+1} (\frac{1}{n^s} - \frac{1}{x^s}) dx$. Les fonctions ϕ_n sont holomorphes sur le demi plan $Re(s) > 0$. De plus pour $s = \sigma + it$, avec $\sigma > 0$, on a :

$$\begin{array}{rcl} |\phi_n(s)| = \left|\int_n^{n+1} (\frac{1}{n^s} - \frac{1}{x^s}) dx\right| & \leq & \sup\limits_{n \leq x \leq n+1} |\frac{1}{n^s} - \frac{1}{x^s}| \\ & = & \sup\limits_{n \leq x \leq n+1} \left|s \int_1^x \frac{1}{t^{s+1}} dt\right| \\ & \leq & \frac{|s|}{n^{\sigma+1}}. \end{array}$$

Ceci implique que la série $\sum \phi_n$ converge normalement vers f_1 sur les sous-ensembles compacts de demi-plan $Re(s) > 0$. D'où f est holomorphe sur le demi-plan $Re(s) > 0$.

Posons $\zeta(s) = \frac{1}{s-1} + f_1(s)$ pour tout $s \neq 1$ avec $Re(s) > 0$. Ce qui donne un prolongement de la fonction ζ sur le demi plan $Re(s) > 0$ avec un pôle simple en $s = 1$. D'après le principe du prolongement analytique ce prolongement est unique.

Ce qui nous fournit une autre démonstration du **Proposition**3.3.1.

prolongement analytique de ζ sur $Re(s) < 0$

On considère la transformation de Fourier d'une fonction $f \in L^1(\mathbb{R})$ par : $\widehat{f}(x) = \int_{-\infty}^{+\infty} f(y) e^{-2i\pi xy} dy$, il est bien connu que $\sum\limits_{n \in \mathbb{Z}} f(n) = \sum\limits_{n \in \mathbb{Z}} \widehat{f}(n)$, pour toute fonction dérivable sur $\mathbb{R}$ vérifiant les deux conditions

- $\sum\limits_{n \in \mathbb{Z}} f(n)$ converge
- $\sum\limits_{n \in \mathbb{Z}} f'(x+n)$ converge uniformément sur [0,1].

la dite formule s'appelle la formule de Poisson.

Les conditions d'application de la formule de Poisson sont satisfaites pour la fonction $f_u(x) =$

$e^{-\pi u x^2}$ pour tout $u > 0$ fixé. on a $\widehat{f_u}(x) = e^{-\frac{\pi x^2}{u}} u^{-1/2}$, et donc la fonction $\mathcal{V} :]0, +\infty[\to]0, +\infty[$ qui à chaque u on associe $\mathcal{V}(u) = \sum_{n\in\mathbb{Z}} f_u(n)$ vérifie l'équation $\mathcal{V}(\frac{1}{u}) = \sqrt{u}\,\mathcal{V}(u)$ pour tout $u > 0$.
La fonction Γ définie par $\Gamma(s) = \int_0^{+\infty} x^{s-1}e^{-x}dx$ pour tout $s \in \mathbb{C}$ tel que $Re(s) > 0$.(Fonction Gamma).
Le théorème de dérivation sous le signe intégrale montre que la fonction Γ est holomorphe sur le demi-plan $Re(s) > 0$. De plus une intégration par partie montre que $\Gamma(s+1) = s\Gamma(s)$. Ce qui permet de prolonger la fonction Γ en une fonction méromorphe sur $\mathbb{C}$, admettant un pôle simple en tout entier négatif et on a les propriétés suivantes

1. $\Gamma(n+1) = n!$;
2. $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$ (formule des compléments) ;
3. $\Gamma(s)\Gamma(s+1/2) = \sqrt{\pi}2^{1-2s}\Gamma(2s)$ (Formule de duplication).

Théorème 3.1.1. *Il existe une équation fonctionnelle de la forme*

$$\zeta(s) = \psi(s)\zeta(1-s), \quad avec \ 0 < Re(s) < 1$$

où $\psi(s)$ est une fonction analytique définie pour tout $s \in \mathbb{C}$ qui n'est pas entier positif impair, définie par : $\psi(s) = 2^s\pi^{s-1}\sin(\frac{1}{2}\pi s)\Gamma(1-s)$

Démonstration. En faisant le changement de variable $x = \pi n^2 y$ dans l'intégrale de définition de $\Gamma(\frac{1}{2}s)$, on obtient pour tout $n \in \mathbb{N}^*$ et $Re(s) > 1$.

$$\Gamma(\frac{s}{2}) = \int_0^{+\infty} x^{(s/2-1)}e^{-x}dx = \pi^{s/2}n^s \int_0^{+\infty} y^{(s/2-1)}e^{-\pi n^2 y}dy$$

ou bien

$$\pi^{-s/2}n^{-s}\Gamma(\frac{s}{2}) = \int_0^{+\infty} y^{(s/2-1)}e^{-\pi n^2 y}dy$$

En sommant sur tous les entiers non nuls, on obtient

$$\zeta(s)\Gamma(\frac{s}{2})\pi^{-s/2} = \int_0^{+\infty} \mathcal{V}_1(y)y^{(s/2-1)}dy$$

où $\mathcal{V}_1(y) = 1/2(\mathcal{V}(y) - 1)$.
Maintenant, on écrit :

$$\zeta(s)\Gamma(\frac{s}{2})\pi^{-s/2} = \int_0^1 \mathcal{V}_1(y)y^{(s/2-1)}dy + \int_1^{+\infty} \mathcal{V}_1(y)y^{(s/2-1)}dy.$$

En effectuant le changement de variable $z = \frac{1}{y}$ sur]0,1] on obtient : $\int_0^1 \mathcal{V}_1(y)y^{(s/2-1)}dy = \int_1^{+\infty} \mathcal{V}_1(1/z)\frac{1}{z^{(s/2+1)}}dz$. D'après ce qui précède, on vérifie facilement que $\mathcal{V}_1(1/z) = \sqrt{z}\,\mathcal{V}_1(z) + 1/2(\sqrt{z}-1)$. ce qui implique que

$$\begin{aligned}\int_0^1 \mathcal{V}_1(y)y^{(s/2-1)}dy &= \int_1^{+\infty} \mathcal{V}_1(z)z^{-(\frac{s+1}{2})}dz + 1/2\int_1^{+\infty}\frac{\sqrt{z}-1}{z^{(s/2+1)}}dz \\ &= \int_1^{+\infty} \mathcal{V}_1(z)z^{-(\frac{s+1}{2})}dz + \frac{1}{s(s-1)}.\end{aligned}$$

D'où

$$\zeta(s)\Gamma(\frac{s}{2})\pi^{-s/2} = \frac{1}{s(s-1)} + \int_1^{+\infty} \mathcal{V}_1(x)(x^{-(\frac{s+1}{2})} - x^{(\frac{s}{2}-1)})dx. \tag{3.2}$$

Puisque $\forall x \geq 1$ on a :

$$\begin{aligned}\mathcal{V}_1(x) = \sum_{n=1}^{+\infty} e^{-\pi n^2 x} &= e^{-\pi x}\sum_{n=1}^{+\infty} e^{-\pi x(n^2-1)} \\ &\leq e^{-\pi x}\sum_{n=0}^{+\infty} e^{-\pi n x} = \frac{e^{-\pi x}}{1-e^{-\pi x}}.\end{aligned}$$

Cela signifie que $\mathcal{V}_1(x) = \mathcal{O}(e^{-\pi x})$. Le théorème de dérivation sous le signe intégrale montre que cette dernière intégrale est holomorphe sur tout le plan complexe et le membre de droite de l'Equation3.2, fournit un prolongement de $\zeta(s)\Gamma(\frac{s}{2})\pi^{-s/2}$ sur $\mathbb{C} \setminus \{0,1\}$ en une fonction analytique invariante par la transformation $s \mapsto 1-s$. pour $0 < Re(s) < 1$ on a donc

$$\zeta(s)\Gamma(\frac{s}{2})\pi^{-s/2} = \zeta(1-s)\Gamma(1/2-s/2)\pi^{(s-1)/2}.$$

En multipliant par $\Gamma(1-s/2)$ il vient que

$$\zeta(s)\Gamma(\frac{1}{2}s)\Gamma(1-s/2) = \zeta(1-s)\Gamma(1/2-s/2)\Gamma(1-s/2)\pi^{(2s-1)/2}.$$

Les formules des compléments et de duplication implique que :

$$\zeta(s) = 2^s\pi^{s-1}\sin(\frac{s}{2}\pi)\Gamma(1-s)\zeta(1-s).$$

D'autre part :
Pour $n \in \mathbb{N}^*$, la formule $\Gamma(s+1) = s\Gamma(s)$ entraîne que $\Gamma(1-s) = \frac{\Gamma(2n+1-s)}{(1-s)(2-s)...(2n-s)}$ en effectuant un développement limité à l'ordre 1 de $\sin(1/2\pi s)$, au voisinage de $2n$ on obtient :

$$\sin(\frac{\pi s}{2}) = \frac{(-1)^n\pi}{2}(s-2n) + o(s-2n).$$

D'où $\lim_{s\to 2n} \sin(\frac{\pi s}{2})\Gamma(1-s) = \frac{(-1)^n\pi}{2(2n-1)!}$. ce qui permet de définir $\psi(s)$ en $s = 2n$ et on a $\psi(2n) = \frac{(-1)^n(2\pi)^{2n}}{2(2n-1)!}$ pour $n \in \mathbb{N}^*$. Donc $\psi(s)$ a un sens pour toute valeur de $s \in \mathbb{C}$ qui n'est pas un entier positif impair.
Ce qui termine la preuve. □

Conséquences

1. L'équation fonctionnelle dans le **Théorème**3.1.1 permet d'écrire pour $s \neq 0$ la formule suivante
$$\zeta(s) = -2^{s-1}\pi^s \frac{\sin(\frac{\pi s}{2})}{\frac{\pi s}{2}}(-s\zeta(1-s))\Gamma(1-s).$$
Puisque $(s-1)\zeta(s)$ tend vers 1 quand s tend vers 1. Donc $-s\zeta(1-s)$ tend vers 1 quand s tend vers 0, et on a également $\lim_{s\to 0}\zeta(s) = -1/2$, d'où ζ est définie en 0 et $\zeta(0) = -1/2$.

2. Pour $n \in \mathbb{N}^*$, en faisant tendre s vers $2n+1$ dans l'identité $\zeta(s) = \psi(s)\zeta(1-s)$ le membre de gauche tend vers une limite finie $\zeta(2n+1)$, et puisque $|\psi(s)| \to +\infty$ alors nécessairement $\zeta(1-s)$ tend vers zéro, cela veut dire que $\zeta(-2n) = 0, \forall n \in \mathbb{N}^*$. Les nombres $2; 4; \ldots$ s'appellent les zéros triviaux de la fonction ζ.

3. Comme la fonction Γ ne s'annule en aucun point du plan complexe, l'équation fonctionnelle permet de conclure que les zéros non triviaux de la fonction ζ se situent sur la bande $0 \leq Re(s) \leq 1$. Or d'après [3] la fonction ζ ne s'annule pas sur $Re(s) = 1$, donc l'équation fonctionnelle entraînent que ζ ne s'annule pas sur la droite $Re(s) = 0$. Par conséquence les zéros non triviaux de ζ sont dans la bande ouverte $0 < Re(s) < 1$, appelée la bande critique.

4. Les zéros triviaux sont les seuls zéros réels de $\zeta(s)$. Pour justifier cela, il suffit de montrer que ζ ne s'annule pas dans l'intervalle]0,1[. On vérifie que pour $Re(s) > 0$ on a $\zeta(s) = \frac{s}{s-1} - s\int_1^{+\infty} \frac{t-E(t)}{t^{s+1}}dt$. Puisque $t - E(t) \in]0,1[$, où $E(t)$ la partie entière de t, on déduit que $\zeta(s) < 0$ pour tout $s \in]0,1[$. Ceci permet de conclure.

5. Les nombres de Bernoulli sont définis comme étant les coefficients du développement de Taylor de $\frac{x}{e^x-1} = \sum_{n=0}^{+\infty} B_n\frac{x^n}{n!}$. On a d'après [4] $\zeta(2n) = (-1)^{n-1}2^{n-1}\frac{B_{2n}}{(2n)!}\pi^{2n}$, $(n \geq 1)$. En particulier : $\zeta(2) = \frac{\pi^2}{6}; \zeta(4) = \frac{\pi^4}{90}; \ldots$

3.1.4 Caractères dans les groupes abeliens

Soit $(G,.)$ un groupe abelien.

Définition 3.1.2. Un caractère de G est un homomorphisme de G dans le groupe des nombres complexes de valeurs absolues 1. L'ensemble des caractères de G est noté par $\widehat{G}$.

Si χ_1, χ_2 deux caractères de G, alors le produit noté $\chi_1\chi_2$ est définie par $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$. Le produit de deux caractères est un caractère. Cette opération fait de $\widehat{G}$ un groupe abelien. L'élément neutre est appelé le **caractère principal**, noté usuellement par χ_0 et satisfait $\chi_0(a) = 1, \forall a \in A$.
L'inverse dans $\widehat{G}$ d'un caractère χ est la fonction $a \to \chi(a)^{-1}$. Le groupe $\widehat{G}$ est appelé le groupe des caractères de G. (Parfois on dit le dual de G).

Proposition 3.1.5. *Si G est un groupe abelien fini alors $\widehat{G} \simeq G$.*

Démonstration. On utilise l'induction sur l'ordre de $G, |G|$.
Supposons que G est cyclique d'ordre m engendré par y. Alors $y^m = 1$ ce qui implique que $\chi_(y)$ est une racine $m^{\text{ième}}$ de l'unité pour tout caractère χ. Fixons une racine primitive $m^{\text{ième}}$ de l'unité ξ. Chaque caractère χ est complètement déterminé une fois $\chi(y)$ est donné. Car $\chi(y^t) = \chi(y)^t$. Pour chaque entier r la fonction définie par $\chi_r(y^j) = (\xi^r)^j$ est un caractère et ces derniers sont différents pour $r = 0,1,\ldots,(m-1)$. De plus $\chi_r = \chi_1^r$, ce qui permet de déterminer la valeur de $\chi(y)$. Donc $\widehat{G}$ est un groupe cyclique engendré par χ_1, car $\chi_1^k(y) = 1$ si et seulement si $\xi^k = 1$. Il s'ensuit que χ_1 est d'ordre m et $\widehat{G}$ cyclique d'ordre m et donc $\widehat{G} \simeq G$.
Maintenant on suppose que $G = G_1 \times G_2$ avec $G_i \neq 1$ et on démontre que $\widehat{G} \simeq \widehat{G_1} \times \widehat{G_2}$. Ainsi le résultat découle facilement du fait que $\widehat{G_i} \simeq G_i$.
On considère l'application ϕ définie par :

$$\begin{array}{rccc} \phi: & \widehat{G} & \to & \widehat{G_1} \times \widehat{G_2} \\ & \chi & \mapsto & \left(\chi_{|\widehat{G_1}}, \chi_{|\widehat{G_2}}\right). \end{array}$$

On a ϕ est bien un homomorphisme de groupes. On définit un homomorphisme de l'autre direction soit ψ par :

$$\begin{array}{rccc} \psi: & \widehat{G_1} \times \widehat{G_2} & \to & \widehat{G} \\ & (\chi_1, \chi_2) & \mapsto & \chi : a_1a_2 \mapsto \chi_1(a_1)\chi_2(a_2). \end{array}$$

On vérifié facilement que $\phi \circ \psi = \psi \circ \phi = id$. C'est à dire ϕ est un isomorphisme et ψ son inverse. D'où le résultat voulu. □

Corollaire 3.1.2. *Si G un groupe abelien fini alors G est naturellement isomorphe à $\widehat{\widehat{G}}$.*

Démonstration. Soit l'application de G dans $\widehat{\widehat{G}}$ qui associée chaque élément $a \in G$ par le caractère de $\widehat{G}$ définie par : $\chi \mapsto \chi(a)$. On vérifie facilement que cette application est un

homomorphisme de groupes. Soit N son noyau, alors pour tout $b \in N$ on a $\chi(b) = 1$, $\forall \chi \in \widehat{G}$. Donc chaque caractère de G peut être vue comme caractère de G/N.
Donc $|G| = |\widehat{G}| \leq |G/N|$, par conséquence $|N| = 1$. Donc l'application est injective et comme leurs ordres son égaux alors elle réalise un isomorphisme. □

Proposition 3.1.6. *Soient G un groupe abélien, χ_1, χ_2 deux caractères de G et a,b deux éléments de G. Alors on a*

1.
$$\sum_{a \in G} \chi_1(a)\chi_2(a) = \begin{cases} 0 & si\ \chi_1 \neq \chi_2^{-1} \\ |G| & si\ \chi_1 = \chi_2^{-1}. \end{cases}$$

2.
$$\sum_{\chi \in \widehat{G}} \chi(a)\chi(b) = \begin{cases} 0 & si\ a \neq b^{-1} \\ |G| & si\ a = b^{-1}. \end{cases}$$

Démonstration. Soit χ un caractère de G non principal et b un élément de G pour lequel $\chi(b) \neq 1$. Alors puisque la somme sur tous $a \in G$ est la même some sur tous les ab. On aura :

$$\sum_{a \in G} \chi(a) = \sum_{a \in G} \chi(ab) = \chi(b) \sum_{a \in G} \chi(a).$$

Puisque $\chi(b) \neq 1$ on tire $\sum\limits_{a \in G} \chi(a) = 0$. On applique le résultat au caractère $\chi = \chi_1\chi_2$, on trouve l'assertion 1.
Pour l'assertion 2., il suffit de remplacer G par $\widehat{G}$ et $\widehat{\widehat{G}}$ par G. par l'identification l'assertion découle. □

3.2 Fonction zeta de Dedekind (Sur un corps de nombres)

Soit K un corps de nombre, A_K (ou A) l'anneau des entiers algébriques de K. Pour chaque idéal entier $\mathcal{U}$ on définit $\mathcal{N}(\mathcal{U})$ comme le générateur positive de l'idéal $N_{K|\mathbb{Q}}(\mathcal{U})$ et ce nombre est égal au cardinal de $A/\mathcal{U}$. Notons que pour chaque $n \in \mathbb{N}^*$, il existe un nombre fini d'idéaux de norme n, noté $a_K(n)$.

Définition 3.2.1. Soient K un corps de nombres et $a_K(n)$ le nombre des idéaux de K de norme l'entier n. On définie la fonction $\zeta = \zeta_K$ sur K par :

$$\zeta_K(s) = \sum_{n=1}^{+\infty} \frac{a_K(n)}{n^s}.$$

La fonction ζ sur K peut être définie par

$$\zeta_K(s) = \sum_{\mathcal{U}\,\text{entier}\neq 0} \frac{1}{\mathcal{N}(\mathcal{U})^s}$$

Remarque 11: La fonction ζ de Riemann est la fonction ζ du corps des nombres rationnels $\mathbb{Q}$. Maintenant soit $\mathfrak{m}$ le module de K et $\mathbf{k}$ une classe modulo $i(K_{\mathfrak{m},1})$ dans le groupe idéal $\mathbb{I}^{\mathfrak{m}}$ on définit la fonction ζ de la classe $\mathbf{k}$ par :

$$\zeta_K(s,\mathbf{k}) = \sum_{\mathcal{U}\in\mathbf{k},\mathcal{U}\,entier} \frac{1}{\mathcal{N}(\mathcal{U})^s}$$

Notons que lorsque $\mathfrak{m} = (1)$ trivial, alors $\mathbb{I}^{\mathfrak{m}} = \mathbb{I}_K$ et $\zeta_K(s) = \sum_{\mathbf{k}} \zeta_K(s,\mathbf{k})$. Écrivons

$$\zeta_K(s,\mathbf{k}) = \sum_n \frac{a(n,\mathbf{k})}{n^s}$$

où $a(n,\mathbf{k})$ est le nombre des idéaux de $\mathbf{k}$ ayant exactement la norme n. Alors $S(n,\mathbf{k}) = a(1,\mathbf{k}) + \ldots + a(n,\mathbf{k})$ est le nombre des idéaux entiers dans $\mathbf{k}$ de normes au plus n.

Théorème 3.2.1. *On garde les mêmes notations. Alors on a :*
La fonction $\zeta_K(s,\mathbf{k})$ est analytique dans la région $Re(s) > 1 - \frac{1}{d}$ sauf pour $s = 1$. Où d est la dimension de K en tant qu'espace vectoriel sur $\mathbb{Q}$, $d = [K : \mathbb{Q}]$.

Démonstration. Pour la preuve voir [[1], page 153]. □

D'après Le **Corollaire**3.1.1, la limite $\lim_{n\to\infty} \frac{S(n,\mathbf{k})}{n} = \lim_{s\to 1}(s-1)\zeta_K(s,\mathbf{k})$.

Théorème 3.2.2. *Soit $\zeta_K(s,\mathbf{k})$ la $\zeta-$fonction de la classe $\mathbf{k}$ de $i(K_{\mathfrak{m},1})$ dans $\mathbb{I}^{\mathfrak{m}}$. Alors*

$$\lim_{s\to 1}(s-1)\zeta_K(s,\mathbf{k}) = g_{\mathfrak{m}} = \frac{2^{r+s}\mathrm{reg}(\mathfrak{m})\pi^s}{\omega_m \mathcal{N}(\mathfrak{m})|\Delta_K|^{\frac{1}{2}}}.$$

où

- $\mathrm{reg}(\mathfrak{m})$ *est régulateur de* $\mathfrak{m}$,
- r *le nombre des premiers réels de* K,
- s *le nombre des premiers complexes de* K,

- $\omega_{\mathfrak{m}}$ *le nombre des racines de l'unité dans* $\mathbb{U}_K \cap K_{\mathfrak{m},1}$,
- Δ *discriminant* $\Delta(A_K/\mathbb{Z})$ *de* A_K *sur* $\mathbb{Z}$.

Démonstration. La preuve se découle du **Théorème**2.2.1 et du **Corollaire**3.1.1. □

Cas particulier

Si $\mathfrak{m} = (1)$ le module trivial, le groupe de classe de rayon $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1})$ est le groupe de classes C_K. Lorsque on prend la some des fonctions ζ des classes, on obtient la fonction ζ de K, soit $\zeta_K(s) = \sum_{\mathbf{k}} \zeta_K(s,\mathbf{k})$. Car l'union des classes $\mathbf{k}$ contient tous les idéaux entiers.
Multipliant par $(s-1)$ et passant à la limite lorsque s tend vers 1.

Théorème 3.2.3. *On garde les mêmes notations alors on a*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r+s}\pi^s \mathrm{reg}(K)}{w_K\sqrt{|\Delta|}}h_K.$$

Où

- w_K *le nombre des racines de l'unité dans* K,
- h_K *le nombre de classes de* K,
- $\mathrm{reg}(K)$ *le régulateur de* K.

Cas d'un corps quadratique

Soit $k = \mathbb{Q}(\sqrt{d})$, avec d un entier relatif sans facteur carré, un corps quadratique. Si $d > 0$ alors $(r = 2; s = 0)$ et si $d < 0$ on a $(r = 0; s = 1)$. Il s'ensuit du **Théorème**3.2.3 que :

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \begin{cases} \frac{2\mathrm{reg}(K)}{w_K\sqrt{|\Delta|}}h_K & \text{si } d > 0 \\ \frac{2\pi\mathrm{reg}(K)}{w_K\sqrt{|\Delta|}}h_K & \text{si } d < 0. \end{cases} \tag{3.3}$$

Pour $d = -3$, on a $\omega_K = 6$ et pour $d = -1$ on a $\omega_K = 4$ quant pour les autres $d < 0$ le nombre $\omega_K = 2$.
Le discriminant vaut d ou $4d$ selon est ce que $d \equiv 1 \bmod 4$ ou non. Plus précisément on a $|\Delta| = D$ avec

$$D = \begin{cases} d & \text{si } d \equiv 1 \bmod 4 \\ 4d & \text{si } d \equiv 2 \,\text{ou}\, 3 \bmod 4. \end{cases}$$

Le régulateur est égale à 1 pour les corps quadratiques imaginaires car les seules unités sont les racines de l'unité. Pour les corps quadratiques réels on sait que le groupe des unités de l'anneau des entiers de K est de la forme $< -1 > \times < u >$ avec u l'unité fondamentale et $u > 1$. Dans ce cas le régulateur est $\mathrm{reg}(K) = \ln u$.
Donc de L'**equation**3.2.3 on en déduit que

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \begin{cases} \frac{2\ln u}{\sqrt{D}} h_K & \text{si } d > 0 \\ \frac{2\pi \mathrm{reg}(K)}{\omega_K \sqrt{D}} h_K & \text{si } d < 0. \end{cases}$$

Il s'ensuit que

$$h_K = \begin{cases} \frac{\sqrt{D}}{2\ln u} \lim_{s\to 1}(s-1)\zeta_K(s) & \text{si } d > 0 \\ \frac{\omega_K \sqrt{D}}{2\pi} \lim_{s\to 1}(s-1)\zeta_K(s) & \text{si } d < 0. \end{cases} \tag{3.4}$$

La formule du nombre de classes d'un corps quadratique.

3.3 $L-$ series et Applications

3.3.1 Généralités sur la fonction L.

Dans cette section nous s'intéressons à une généralisation de la fonction ζ. Soit K un corps de nombres, $\mathfrak{m}$ un module de K et χ un caractère du groupe abélien fini $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1})$. On regarde χ comme un caractère de $\mathbb{I}^{\mathfrak{m}}$ avec $i(K_{\mathfrak{m},1})$ contenu dans son noyau. $\chi(\mathcal{U})$ est la valeur de χ en $\mathcal{U}i(K_{\mathfrak{m},1})$.

Définition 3.3.1. Soient $\mathfrak{m}$ un module et χ un caractère du $\mathbb{I}^{\mathfrak{m}}/i(K_{\mathfrak{m},1})$. La $L-$série pour χ et $\mathfrak{m}$ est définie par

$$L(s,\chi) = \sum_{\mathcal{U}\in\mathbb{I}^{\mathfrak{m}},\mathcal{U}\,\text{entier}} \frac{\chi(\mathcal{U})}{\mathcal{N}(\mathcal{U})^s}.$$

où la somme porte sur tous les idéaux entiers premiers à $\mathfrak{m}$.

Exemple 3.3.1. On a d'après les **Exemples**2.1.1, pour $\mathfrak{m} = (D)\infty$ on a $\mathbb{I}_{\mathbb{Q}}^{(\mathfrak{m})}/i(\mathbb{Q}_{\mathfrak{m},1}) \sim (\mathbb{Z}/D\mathbb{Z})^*$. Les caractères sur $\mathbb{I}_{\mathbb{Q}}^{(D)}/i(\mathbb{Q}_{D,1})$ peuvent être vue comme caractère sur $(\mathbb{Z}/D\mathbb{Z})^*$. De plus on vérifie plus loin que $\chi(n+D) = \chi(n)$.
Pour $D = 10$, on a $(\mathbb{Z}/D\mathbb{Z})^* = \{1,3,7,9\}$, on aura $\chi(1) = 1, \chi(3) = i, \chi(7) = -i$ et $\chi(9) = -1$. Donc

$$L(s,\chi) = 1 + \frac{i}{3^s} - \frac{i}{7^s} - \frac{1}{9^s} + \frac{1}{11^s} + \frac{i}{13^s} - \frac{i}{15^s} - \frac{1}{19^s} + \dots$$

Remarque 12: Puisque $\chi(\mathcal{U})$ dépend uniquement des classes $\mathbf{k}$ de $\mathcal{U}$, on peut exprimer $L(s,\chi)$ en termes de la fonction $\zeta(s,\mathbf{k})$.

$$L(s,\chi) = \sum_{\mathbf{k}} \chi(\mathbf{k}) \sum_{\mathcal{U}\in\mathbf{k},\mathcal{U}\,\text{entier}} \mathcal{N}(\mathcal{U})^{-s} = \sum_{\mathbf{k}} \chi(\mathbf{k})\zeta(s,\mathbf{k}) \tag{3.5}$$

Proposition 3.3.1. *On garde les mêmes notations de la* ***Définition****3.3.1. Alors on a*

$$\lim_{s\to 1}(s-1)L(s,\chi) = \begin{cases} 0 & si\ \chi \neq \chi_0 \\ h_m g_m & si\ \chi = \chi_0. \end{cases}$$

où h_m est l'ordre du groupe de classes de rayon et g_m est la constante définie dans le ***Théorème****3.2.2.*

Démonstration. Par L'**équation**3.5 on obtient

$$\lim_{s\to 1}(s-1)L(s,\chi) = \sum_{\mathbf{k}} \chi(\mathbf{k}) g_m.$$

Le résultat se découle en applicant les propriétés de l'orthogonalité **Proposition**3.1.6. □

Théorème 3.3.1. *On garde les mêmes notations. Alors pour tout $s \in \mathbb{C}$ avec $Re(s) > 1$, la fonction $L(s,\chi)$ peut s'exprimer par un produit infini uniformément convergeant comme suit*

$$L(s,\chi) = \prod_{\mathcal{P}|\mathfrak{m}} \left(1 - \frac{\chi(\mathcal{P})}{\mathcal{N}(\mathcal{P})^s}\right)^{-1}.$$

Le produit est pris sur tous les idéaux premiers ne divisant pas le module $\mathfrak{m}$.

Démonstration. Soit $\mathcal{P}$ un idéal premier, la série

$$\left(1 - \frac{\chi(\mathcal{P})}{\mathcal{N}(\mathcal{P})^s}\right)^{-1} = 1 + \frac{\chi(\mathcal{P})}{\mathcal{N}(\mathcal{P})^s} + \frac{\chi(\mathcal{P}^2)}{\mathcal{N}(\mathcal{P}^2)^s} + \dots$$

est absolument convergente.
Soient t un entier positif et $\mathcal{P}_1,\dots,\mathcal{P}_r$ tous les premiers de $\mathbb{I}^{\mathfrak{m}}$ et de normes inférieure ou égale à t. Donc

$$\prod_{i=1}^{r}\left(1 - \frac{\chi(\mathcal{P}_i)}{\mathcal{N}(\mathcal{P}_i)^s}\right)^{-1} = \sum_{a_i\geq 0} \frac{\chi(\mathcal{P}_1^{a_1}\dots\mathcal{P}_r^{a_r})}{\mathcal{N}(\mathcal{P}_1^{a_1}\dots\mathcal{P}_r^{a_r})^s} = \sum_{\mathcal{U}} \frac{\chi(\mathcal{U})}{\mathcal{N}(\mathcal{U})^s}.$$

Où $\mathcal{U}$ parcourt les idéaux divisible uniquement par les premiers de $\mathbb{I}^{\mathfrak{m}}$ de normes au plus t.
Les idéaux entiers dans $\mathbb{I}^{\mathfrak{m}}$ divisible par les premiers ayant la norme supérieure à t forment

un sous-ensemble de l'ensemble des idéaux ayant la norme supérieure à t. Il s'ensuit de la définition de la $L-$série que

$$\left| L(s,\chi) - \prod_{\mathcal{N}(\mathcal{P})\leq t} \left(1 - \frac{\chi(\mathcal{P})}{\mathcal{N}(\mathcal{P})^s}\right)^{-1} \right| \leq \sum_{\mathcal{N}(\mathcal{U})>t} \left| \frac{\chi(\mathcal{U})}{\mathcal{N}(\mathcal{U})^s} \right|$$

or $|\chi(\mathcal{U})| = 1$, le terme qui reste est le reste de la série ζ_K. Puisque ζ_K converge uniformément pour $Re(s) > 1$, le reste tend vers 0 lorsque t tend vers $+\infty$. D'où le résultat. □

Corollaire 3.3.1. *Pour* $\mathfrak{m} = (1)$ *et* $\chi = \chi_0$ *alors* $L(s,\chi_0) = \zeta_K(s)$ *et on a*

1. $\zeta_K(s) = \prod_{\mathcal{P}} (1 - \mathcal{N}(\mathcal{P})^{-s})^{-1}$, *où* $\mathcal{P}$ *parcourt tous les idéaux premiers de* A_K.
2. $\zeta_{\mathbb{Q}}(s) = \prod_{p} (1 - p^{-s})^{-1}$, *où* p *parcours tous les nombres premiers. (Formule d'Euler) (**Proposition**3.1.4).*

Conséquences

Du **Corollaire**3.3.1 et **Proposition**3.3.1, on en déduit que

1. $Log(\zeta_K(s)) = \sum_{\mathcal{P}} \mathcal{N}(\mathcal{P})^{-s} + g_1(s)$
2. $Log(\zeta_{\mathbb{Q}}(s)) = \sum_{p} p^{-s} + g_2(s)$.

Où g_1 et g_2 sont bornées en $s = 1$ et les sommes portent sur tous les premiers de A_K respectivement sur tous les premiers de $\mathbb{N}$.

Remarque 13: L'équation $Log(\zeta_{\mathbb{Q}}(s)) = \sum_{p} p^{-s} + g_2(s)$ implique l'existence d'une infinité de nombres premiers. Car s'il existe uniquement un nombre fini de premiers alors $Log(\zeta_{\mathbb{Q}}(s))$ est bornée au voisinage de $s = 1$ et d'après la **Proposition**3.1.2, la fonction $(s-1)\zeta_{\mathbb{Q}}(s)$ est bornée au voisinage de 1. Il s'ensuit que $Log(s-1) = Log((s-1)\zeta_{\mathbb{Q}}(s)) - Log(\zeta_{\mathbb{Q}}(s))$ est bornée en $s = 1$. Ce qui n'est pas vrai, car $-Log(s-1)$ converge vers $+\infty$ lorsque s converge vers 1 suivant la direction de l'axe réel à droite. D'où l'existence d'une infinité de nombres premiers.

Soient $f_1(s)$ et $f_2(s)$ deux fonctions définies sur $Re(s) > 1$. On écrit $f_1(s) \sim f_2(s)$ pour dire $f_1(s) - f_2(s)$ admet une limite fini lorsque s s'approche de 1.

Proposition 3.3.2. *Soit* K *un corps de nombres. Il existe une infinité d'idéaux premiers de* A_K *de degré relative* 1 *sur* $\mathbb{Q}$.

Démonstration. Soient S l'ensemble des idéaux premiers de A_K ayant le degré 1 sur $\mathbb{Q}$ et S' son complémentaire dans l'ensemble des idéaux premiers. D'après le **Corollaire**3.3.1 on tire

$$Log(\zeta_K(s)) \sim \sum_{\mathcal{P}} \frac{1}{\mathcal{N}(\mathcal{P})^s} = \sum_{\mathcal{P}\in S} \frac{1}{\mathcal{N}(\mathcal{P}^s)} + \sum_{\mathcal{P}\in S'} \frac{1}{\mathcal{N}(\mathcal{P}^s)}$$

Pour chaque premier $\mathcal{P} \in S$, on a $\mathcal{N}(\mathcal{P}) = p$, p premier. Pour $\mathcal{P} \in S'$ on a $\mathcal{N}(\mathcal{P}) = p^f \geq p^2$. Maintenant on estime la somme sur S'.
Du fait qu'il existe au plus $[K : \mathbb{Q}]$ premiers de A_K ayant la norme une puissance de p donc

$$|\sum_{\mathcal{P}\in S'} \frac{1}{\mathcal{N}(\mathcal{P}^s)}| \leq [K : \mathbb{Q}] \sum_{p} \frac{1}{p^{2\sigma}}, \;\; \sigma = Re(s)$$

La somme sur S' est bornée car $\zeta_Q(2)$ est fini (σ au voisinage de 1). On conclut que

$$Log(\zeta_K(s)) \sim \sum_{\mathcal{P}\in S} \frac{1}{\mathcal{N}(\mathcal{P}^s)}.$$

De la **Proposition**3.1.1, on a $(s-1)\zeta_K(s)$ est bornée en $s = 1$. par passage à la limite vers 1 suivant la direction (Ox) à droite de 1 on obtient $Log(\zeta_K(s)) \sim -Log(s-1)$ ce qui entraîne que $-Log(s-1) \sim \sum_{\mathcal{P}\in S} \frac{1}{\mathcal{N}(\mathcal{P}^s)}$ □

3.3.2 Applications aux corps quadratiques

Caractère du corps quadratique

Soit $K = \mathbb{Q}(\sqrt{d})$, où D un entier sans facteur carré, un corps quadratique. On définit le caractère quadratique $\chi = \chi_K$ sur K par ses valeurs dans $\{0,1,-1\}$ par :

$$\chi(p) = \begin{cases} 1 & \text{si } pA_K = \mathcal{P}_1\mathcal{P}_2 \;\; (p \text{ se décompose dans } \;\; K) \\ -1 & \text{si } pA_K = \mathcal{P} \;\; (p \text{ inerte dans } \;\; K) \\ 0 & \text{si } pA_K = \mathcal{P}^2. \;\; (p \text{ se ramifie } K) \end{cases}$$

Pour $n = \prod_i p_i^{a_i}$, on définit $\chi(n)$ par : $\chi(n) = \prod_i \chi(p_i)^{a_i}$. On remarque que $\chi(n) = 0$ lorsque $\gcd(n,\Delta_K) \neq 1$ et que pour tout entiers non nuls m et n on a $\chi(m)\chi(n) = \chi(mn)$.

Déterminons la relation entre χ_K et le caractère du groupe des unités de $\mathbb{Z}/D\mathbb{Z}$.

Proposition 3.3.3. *Soit ϕ l'application d'Artin pour l'extension $K/\mathbb{Q}$ dont les valeurs sont dans le groupe de Galois* $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$ *, avec* $\sigma^2 = 1$.

Alors Pour chaque entier n premier avec D on a :

$$\phi((n)) = \sigma \Leftrightarrow \chi_K(n) = -1.$$

En particulier, pour tout entier positif n on a : $\chi_K(n+D) = \chi_K(n)$. *De plus si M est un entier positif pour lequel* $\chi_K(n+M) = \chi_K(n)$ *pour tout n premier à D, alors* $D|M$.

Démonstration. La partie fini du conducteur de l'extension K est (D) et l'application d'Artin est un homomorphisme de $\mathbb{I}_{\mathbb{Q}}^{(D)}$ dans $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$ de noyau $i(\mathbb{Q}_{D,1})$. Puisque $\mathbb{I}_{\mathbb{Q}}^{(D)}/i(\mathbb{Q}_{D,1}) \simeq (\mathbb{Z}/D\mathbb{Z})^*$ le groupe des unités de $\mathbb{Z}/D\mathbb{Z}$.
On peut voir ϕ comme homomorphisme définie sur $(\mathbb{Z}/D\mathbb{Z})^*$, et par l'extension naturelle on peut définir ϕ sur les entiers premiers à D par $\phi(n) = \phi((n))$ où (n) est l'idéal engendré par n. Pour un premier de $\mathbb{Z}$, par les propriétés de l'application d'Artin, on a $\phi(p) = \sigma$ si et seulement si pA_K est un idéal premier de l'anneau des entiers de K. Or ceci est réalisé si $\chi_K(p) = -1$. Puisque ϕ et χ_K sont multiplicative, alors la propriété s'étend à tous les entiers premiers à D. Comme ϕ est constante sur chaque classe résiduel, on déduit que $\chi_K(n+kD) = \chi_K(n)$, $\forall k$ tel que $n + kD > 0$ et $\gcd(n,D) = 1$.
Maintenant, supposons que M est un entier positif tel que $\chi_K(n+M) = \chi_K(n)$ pour tout n positif premier à D. Alors pour tout premier $p \equiv 1 \bmod M$, on a $\phi(p) = 1$, car $\chi_K(1+kM) = \chi_K(1) = 1$. Donc chaque $p \equiv 1 \bmod M$ se décompose complètement dans K. Les premiers qui se décomposent dans $\mathbb{Q}(\beta_M)$ où β_M est une racine primitive M^{ieme} de l'unité sont ceux $\equiv 1 \bmod M$. D'où tous les premiers qui se décomposent dans $\mathbb{Q}(\beta_M)$ aussi se décompose dans K. Il s'ensuit de [Corollaire 5.5,chap4,[1]] que $K \subset \mathbb{Q}(\beta_M)$ et donc le conducteur de $\mathbb{Q}(\beta_M)$ sur $\mathbb{Q}$, qui vaut $(M)\mathcal{P}_\infty$, est divisible par celui de K. Donc $D|M$. □

Théorème 3.3.2. *Soit* $\chi = \chi_K$ *le caractère quadratique définie sur* $K = \mathbb{Q}(\sqrt{D})$ *alors :*

$$\chi(D-1) = \begin{cases} 1 & si\ D > 0 \\ -1 & si\ D < 0. \end{cases}$$

Démonstration. On sait que $\chi_K(D-1) = 1 \Leftrightarrow \phi_{K|\mathbb{Q}}(D-1) = 1$ ceci est équivalent à $res_K \phi_{\mathbb{Q}(\beta_D)|\mathbb{Q}}(D-1) = 1$.
l'application d'Artin sur l'extension cyclotomique $\mathbb{Q}(\beta_D)$ envoie $D-1$ sur l'homomorphisme $\sigma : \beta_D \mapsto \beta_D^{D-1} = \beta_D^{-1} = \overline{\beta_D}$.
Le corps fixé par σ est $\mathbb{Q}(\beta_D + \overline{\beta_D})$ qui est le sous corps réel maximal de $\mathbb{Q}(\beta_D)$. D'où la restriction de σ à K est l'identité si et seulement si K est réel. c'est à dire $D > 0$.

On peut étendre le domaine de χ à tous les entiers non nuls par le règle suivante

$$\chi(-1) = \begin{cases} 1 & \text{si } D > 0 \\ -1 & \text{si } D < 0. \end{cases}$$

Et on a $\chi(-n) = \chi(-1)\chi(n)$. □

Relation entre Fonction ζ et Fonction L

Soit $\zeta_K(s) = \sum_{\mathcal{U}} \frac{1}{\mathcal{N}(\mathcal{U})^s} = \prod_{\mathcal{P}} (1 - \mathcal{N}(\mathcal{P})^{-s})^{-1}$ avec la somme est prise sur tous les idéaux entiers de K et $\mathcal{P}$ parcourt les idéaux premiers de l'anneaux des entiers de K.
On exprime la fonction $\zeta_K(s)$ en termes de la fonction ζ de Riemann (sur $\mathbb{Q}$) et la fonction L sur $\mathbb{Q}$ correspondant au caractère quadratique.

Proposition 3.3.4. *Soient K un corps quadratique et χ son caractère quadratique alors pour tout s tel que $Re(s) > 1$ on a :*

$$\zeta_K(s) = \zeta_{\mathbb{Q}}(s)L(s,\chi)$$

où ζ_K la fonction ζ sur K et $\zeta_{\mathbb{Q}}(s) = \zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ la fonction ζ de Riemann et $L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$ est la L−fonction définie sur $\mathbb{Q}$.

Démonstration. Chaque premier de K admet une norme un premier rationnel ou le carré d'un nombre premier rationnel. De plus ceux de normes égales à un premier peuvent être ramifiés on non sur $\mathbb{Q}$.
On écrit la représentation produit de ζ_K comme produit indexés par les premiers rationnels.
La contribution au produit qui correspond à un premier donne

$$\begin{cases} (1 - p^{-2s})^{-1} & \text{si } p \text{ est inerte dans } K, \\ (1 - p^{-s})^{-2} & \text{si } p \nmid D \text{ se décompose dans } K, \\ (1 - p^{-s})^{-1} & \text{si } p = \mathcal{P}^2 \text{ ramifie dans } K \ (p|D). \end{cases}$$

Ces trois expressions peuvent s'écrire sans séparation des cas comme suit :
$(1 - \frac{1}{p^s})^{-1}(1 - \frac{\chi(p)}{p^s})^{-1}$, car la définition de χ utilise les mêmes distinctions.
Il s'ensuit que $\zeta_K(s)$ peut être exprimé comme produit de deux fonctions définie sur $\mathbb{Q}$.
$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ et $L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$. D'après la **Proposition**3.1.3, la représentation produit est valide lorsque $Re(s) > 1$. Donc pour tout s tel que $Re(s) > 1$ on a $\zeta_K(s) = \zeta(s)L(s,\chi)$. □

Remarque 14: La représentation produit convergent uniformément dans chaque région fermé dans le demi plan $Re(s) > 1$ ceci découle de la **Proposition**3.1.3 et **Proposition**3.1.1, car $\sum_{n<x} \chi(n)$ est borné (χ est périodique et nulle sur chaque période).
La $L-$fonction est continue sur $Re(s) > 0$.

Proposition 3.3.5. *On garde les mêmes notations et conditions alors on a :*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = L(1,\chi).$$

Démonstration. On a d'après la **Proposition**3.1.2 que $\lim_{s\to 1}(s-1)\zeta(s) = 1$. Comme $L(s,\chi)$ est continue sur $Re(s) > 0$ et en vertu de la **Proposition**3.3.4 on en déduit que

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \lim_{s\to 1}(s-1)\zeta(s) \times \lim_{s\to 1} L(s,\chi) = 1 \times L(1,\chi) = L(1,\chi).$$

□

Corollaire 3.3.2. *Si χ un caractère quadratique de $K = \mathbb{Q}(\sqrt{d})$. Alors le nombre de classes de K est donné par*

$$h_K = \begin{cases} \frac{\sqrt{D}}{2\ln u} L(1,\chi) & si\ d > 0 \\ \frac{\omega_K\sqrt{D}}{2\pi} L(1,\chi) & si\ d < 0 \end{cases}$$

où $D = |\Delta_K|$ avec Δ_K le discriminant de K et u l'unité fondamentale (> 1) du corps K et ω_K le nombre des racines de l'unité de K.

Démonstration. Le résultat se découle facilement de l'**Equation**3.4. □

3.3.3 Détermination de $L(1,\chi)$

Théorème 3.3.3. *Soient $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique, χ un caractère quadratique et $\gamma = \gamma_D$ la racine primitive D^{ieme} de l'unité. Soit $\mathfrak{g}(\chi,\gamma^j) = \sum_{m=0}^{D-1} \chi(m)\gamma^{mj}$ la somme de Gauss. Alors*

1. *Si $\chi(-1) = 1$ alors $L(1,\chi) = -\frac{2}{D}\mathfrak{g}(\chi,\gamma) \sum_{j=1,\, gcd(j,D)=1}^{D/2} \chi(j)\ln(\sin\frac{\pi j}{D})$*

2. *Si $\chi(-1) = -1$ alors $L(1,\chi) = \frac{i\pi\mathfrak{g}(\chi,\gamma)}{D^2} \sum_{j=0}^{D-1} \chi(j)j$*

Démonstration. On a $L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s} = \sum_{m=0}^{D-1} \chi(m) \sum_{n\geq 1;\, n\equiv m \bmod D} \frac{1}{n^s}$. Or $\sum_{n\geq 1;\, n\equiv m \bmod D} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{C_m(n)}{n^s}$, où $C_m(n) = 0$ si $n \not\equiv m \bmod D$ et $C_m(n) = 1$ sinon.

On donne une expression à ces coefficients comme suit. Soit $\gamma = \gamma_D$ la racine primitive D^{ieme} de l'unité, alors $C_m(n) = \frac{1}{D}\sum_{j=0}^{D-1} \gamma^{(m-n)j}$.
On réécrire la formule $L(s,\chi)$ comme suit

$$\begin{aligned} L(s,\chi) &= \sum_{m=0}^{D-1} \chi(m) \sum_{n=1}^{\infty} \frac{C_m(n)}{n^s} \\ &= \sum_{m=0}^{D-1} \chi(m) \sum_{n=1}^{\infty} \frac{1}{D} \sum_{j=0}^{D-1} \frac{\gamma^{-nj}\gamma^{(m-n)j}}{n^s} \\ &= \frac{1}{D} \sum_{j=0}^{D-1} \sum_{m=0}^{D-1} (\chi(m)\gamma^{mj}) \sum_{n=1}^{\infty} \frac{\gamma^{-nj}}{n^s}. \end{aligned}$$

Donc $L(s,\chi) = \frac{1}{D}\sum_{j=0}^{D-1} \mathfrak{g}(\chi,\gamma^j) \sum_{n=1}^{\infty} \frac{\gamma^{-nj}}{n^s}$.
Posons $l(s) = \sum_{n=1}^{\infty} \frac{\gamma^{-nj}}{n^s}$. D'autre part on a la série $\sum_{n\geq 1} z^n$ converge pour $|z| < 1$. lorsque z est une racine de l'unité mais $z \neq 1$. La série converge car c'est la valeur en $s = 1$ de la série de Dirichlet $\sum \frac{z^n}{n^s}$ qui converge pour s satisfaisant $Re(s) > 0$. (on applique la **Proposition**3.1.1). Donc $Log(1-z)$ est définie et continue lorsque $z = \gamma$ et l'égalité est vérifiée pour les puissances de γ.
Pour $z = \gamma^{-1}$ la série $-\sum \frac{z^n}{n}$ converge vers la valeur principale de $Log(1-\gamma^{-j})$, donc $l(1) = \sum_{n\geq 1} \frac{\gamma^{-nj}}{n} = -Log(1-\gamma^{-j})$.
On obtient les expressions suivantes pour la valeur de L en $s = 1$. On a

$$L(1,\chi) = -\frac{1}{D}\sum_{j=0}^{D-1} \mathfrak{g}(\chi,\gamma^j) Log(1-\gamma^{-j}).$$

Or d'après les propriétés de la somme de Gauss on a $\mathfrak{g}(\chi,\gamma^j) = \chi(j)\mathfrak{g}(\chi,\gamma)$. Il s'ensuit que

$$L(1,\chi) = -\frac{1}{D}\mathfrak{g}(\chi,\gamma)\sum_{j=0}^{D-1} \chi(j) Log(1-\gamma^{-j}).$$

Posons $S = \sum_{j=0}^{D-1} \chi(j) Log(1-\gamma^{-j})$. Évaluons S.
Soit $\gamma = e^{2i\pi/D} = \cos(2\pi/D) + i\sin(2\pi/D)$. Pour $0 < j < D$ on a : $1-\gamma^{-j} = \gamma^{-j/2}(\gamma^{j/2} - \gamma^{-j/2}) = 2i\gamma^{-j/2} = 2i\gamma^{-j/2}\sin\frac{j\pi}{D} = 2\sin\frac{\pi j}{D}\exp(i(\frac{\pi}{2} - \frac{\pi j}{D}))$. Donc la principale valeur du Log est $Log(1-\gamma) = ln|1-\gamma^{-j}| + (\pi/2 - \pi j/D)i$.
Pour le cas $\chi(-1) = 1$:

La valeur de S reste inchangé si on remplace j par $D-j$ et on a :

$$\begin{aligned} S &= \sum_{j=0}^{D-1} \chi(j) Log(1-\gamma^{-j}) = \sum_{j=0}^{D-1} \chi(-j) Log(1-\gamma^{j}) \\ &= \chi(-1) \sum_{j=0}^{D-1} \chi(j) Log(1-\gamma^{j}) = \sum_{j=0}^{D-1} \chi(j) Log(1-\gamma^{j}). \end{aligned}$$

Donc $2S = \sum_{j=0}^{D-1} \chi(j) \left(Log(1-\gamma^{j}) + Log(1-\gamma^{-j})\right)$.
Comme $1-\gamma^{j}$ et $1-\gamma^{-j}$ sont conjugués, alors ils ont le même module et des arguments opposés. D'où $Log(1-\gamma^{j}) + Log(1-\gamma^{-j}) = 2\ln|1-\gamma^{j}| = 2\ln(2\sin\frac{\pi j}{D})$

Par conséquence $S = \sum_{j=0}^{D-1} \chi(j)\ln(2\sin\frac{\pi j}{D})$. or $\sum \chi(j)\ln(2) = 0$, car χ n'est pas un caractère principal, et on élimine l'indice $j=0$ car $\chi(0)=0$. Donc

$$L(1,\chi) = -\frac{1}{D}\mathfrak{g}(\chi,\gamma) \sum_{j=0}^{D-1} \chi(j)\ln(\sin\frac{\pi j}{D}).$$

D'autre part, puisque $\sin(\pi-\alpha) = \sin\alpha$, $\chi(-j) = \chi(j)$ et $\chi(D-j) = \chi(j)$ alors $L(1,\chi)$ devient

$$L(1,\chi) = -\frac{1}{D}\mathfrak{g}(\chi,\gamma) \sum_{0\le j\le D/2,\, gcd(j,D)=1} \chi(j)\ln(\sin\frac{\pi j}{D}).$$

Pour l'assertion 2., On procède comme dans le premier cas on aura $S = -\sum_{j=0}^{D-1} \chi(j) Log(1-\gamma^{j})$ et on tire que $2S = \sum_{j=0}^{D-1} \chi(j)\left(Log(1-\gamma^{-j}) - Log(1-\gamma^{j})\right) = 2\sum_{j=0}^{D-1} \chi(j)\left(\pi/2 - \frac{j\pi}{D}\right) i = -\frac{2i\pi}{D}\sum_{j=0}^{D-1} \chi(j) j$. On en déduit que

$$L(1,\chi) = \frac{\pi i \mathfrak{g}(\chi,\gamma)}{D^2} \sum_{j=0}^{D-1} \chi(j) j$$

D'où le résultat voulu. □

Remarque 15: Lorsque $\chi(-1) = 1$, Si D est pair, alors le terme qui correspond à $j = D/2$ dans l'expression de $L(1,\chi)$ ne sera pas compté et ceci n'influence pas sur le résultat car $\chi(D/2) = 0$. Dans ce cas D doit être différent de 2.

Théorème 3.3.4. *Soit $K = \mathbb{Q}\left(\sqrt{d}\right)$ un corps quadratique et χ son caractère. Alors le nombre*

de classes de K est donné par une des relations suivante :

$$h_K = \begin{cases} \frac{1}{\ln u} \left| \sum_{1\leq j\leq D/2,\,(gcd(j,D)=1)} \chi(j)\ln(\sin\frac{j\pi}{d}) \right| & si\ d>0 \\ \frac{\omega_K}{2D} \left| \sum_{1\leq j<D,\,gcd(j,D)=1} \chi(j)j \right| & si\ d<0. \end{cases}$$

Démonstration. Le Théorème découle du fait que $|g(\chi,\gamma)| = \sqrt{D}$ (Voir[2], ou annexe [1] propriété des sommes de Gauss) et du **Corollaire**3.3.2. □

3.3.4 Exemples

Exemple 3.3.2. On considère $K = \mathbb{Q}(\sqrt{5})$. Pour $d = 5$, on a $D = 5$. Le caractère est définie sur les unités de $\mathbb{Z}/5\mathbb{Z}$ qui est un groupe cyclique d'ordre 4. On a $\chi(2) = -1$ car 2 est inerte dans K. Donc $h_K = \frac{1}{\ln u}|\ln(\sin\frac{\pi}{5}) - \ln(\sin\frac{2\pi}{5})|$. Soit $\xi = e^{2i\pi/5}$ une racine 5^{ieme} de l'unité. Donc

$$\frac{\sin(2\pi/5)}{\sin\pi/5} = \frac{\xi^2 - \overline{\xi}^2}{\xi - \overline{\xi}} = \xi + \overline{\xi}.$$

Or le polynôme minimal de $\xi+\overline{\xi}$ est X^2+X-1 qui a une seule racine positive $v = \frac{-1+\sqrt{5}}{2}$. Notons que cet élément est un entier algébrique de norme -1, donc c'est une unité de A_K comprise entre 0 et 1. D'où $h_K = \frac{|\ln v|}{\ln u} = -\frac{\ln v}{\ln u}$. Où u est l'unité fondamentale de K, $u = v^{-1}(> 1)$. Par conséquence $h = 1$.

Exemple 3.3.3. On détermine le nombre de classes de $K = \mathbb{Q}(\sqrt{-5})$. On a $D = 20$. les valeurs du caractère sont déterminés en un premier p par l'examination de la décomposition de p dans K. Or $\chi(3) = \chi(7) = 1$ car 3 et 7 se décomposent complètement dans K. De plus $\chi(-1) = -1$. Ce qui détermine toutes les valeurs de χ. Plus précisément $\chi(1) = \chi(3) = \chi(7) = \chi(9) = 1$ et $\chi(-9) = \chi(-7) = \chi(-3) = \chi(-1) = -1$. Aussi on a $\omega_K = 2$. Il s'ensuit que $h_K = 2/2 * 20|(1+3+7+9) - (11+13+17+19)| = 2$

Exemple 3.3.4. On considère le corps $K = \mathbb{Q}(\sqrt{-23})$. On aura $\chi(2) = 1$ car 2 est d'ordre 11 modulo 23. L'automorphisme de Frobenius de (2) opère trivialement dans le sous-corps quadratique de $\mathbb{Q}(\xi_{23})$ qui est K, et donc (2) se décompose dans K. Puisque 2 doit être un carré modulo 23 (ou tout simplement car $-23 \equiv 1 \bmod 8$). Alors ses 11 différentes puissances sont des carrés non nuls. Le caractère quadratique est un caractère réel non principal d'un groupe cyclique d'ordre 22 et il est unique. Donc $\chi(n) = 1 \Leftrightarrow n = 2^s \bmod 23$ on obtient : $\sum_{1\leq j\leq 22} \chi(j)j = (1+2+3+4+6+8+9+12+13+16+18) - (5+7+10+11+14+15+$

$17 + 19 + 20 + 21 + 22) = 92 - 161 = -69.$
Donc $h_k = 2/2 * 23| - 69| = 3.$

Chapitre 4

Densité et Progression Arithmétique

4.1 Densité

K désigne un corps de nombres et A_K désigne son anneau des entiers.

4.1.1 Définition et propriétés

Définition 4.1.1. Soit S un ensemble d'idéaux premiers de l'anneau des entiers algébriques A_K, s'il existe un nombre réel δ tel que

$$-\delta Log(s-1) \sim \sum_{\mathcal{P}} \frac{1}{\mathcal{N}(\mathcal{P})^s}$$

On dit que δ est la densité de Dirichlet de S et en écrit $\delta(S) = \delta$.

Exemple 4.1.1. Si S_1 est l'ensemble des idéaux ayant le degré résiduel égal à 1 sur $\mathbb{Q}$ alors $\delta(S_1) = 1$. (Voir Chapitre 3, **Proposition**3.3.2).

4.1.2 propriétés

propriété 1

Soit S un ensemble des idéaux premiers de A_K admettant une densité alors $\delta(S) = \delta(S \cap S_1)$. En effet l'estimation est basée sur $\mathcal{N}(\mathcal{P}) = \mathcal{P}^f \geq p^2$. Pour $\mathcal{P} \in S$ et $\mathcal{P} \notin S_1$. On reprend la preuve de la **Proposition**3.3.2 pour prouver que $\sum_{\mathcal{P}\in S, \mathcal{P}\notin S_1} \mathcal{N}(\mathcal{P}^{-s}) \sim 0$. Il s'ensuit que $\sum_{\mathcal{P}\in S} \mathcal{N}(\mathcal{P}^{-s}) \sim \sum_{\mathcal{P}\in S\cap S_1} \mathcal{N}(\mathcal{P}^{-s})$

Propriété 2

Tout ensemble S des idéaux premiers de A_K admettant une densité de Dirichlet non nulle ($\delta(S) \neq 0$) est infini.

En effet : Si S est fini, alors $\sum_{\mathcal{P}\in S} \mathcal{N}(\mathcal{P}^{-s}) \sim 0$, ce qui implique que $\delta(S) = 0$.

Propriété 3

Soient S et S' deux ensembles des idéaux premiers de K admettant des densités de Dirichlet. Si $S \subset S'$ alors $\delta(S) \leq \delta(S')$.
En effet : $\sum_{\mathcal{P}\in T} \mathcal{N}(\mathcal{P}^{-s})$ avec $T = S' \setminus S$, ne peut pas être négative lorsque s est suffisamment proche de 1.

Propriété 4

Soit S un ensemble des idéaux premiers de A_K qui admet une densité de Dirichlet alors $0 \leq \delta(S) \leq 1$.
En effet : On peut remplacer S par $S \cap S_1$ sans changement de densité et $\delta(S) = \delta(S \cap S_1) \leq \delta(S_1) = 1$ (**Propriété**4.1.2 et **Propriété**4.1.2). La densité ne peut pas être négative car la fonction $\sum \mathcal{N}(\mathcal{P})^{-s}$ prend des valeurs positives lorsque s tend vers 1 adroite de 1 suivant l'axe (Ox).

4.1.3 Densité des premiers dans le groupe de classes de rayon

Soient $\mathfrak{m}$ un module de K et H un sous groupe de $\mathbb{I}^{\mathfrak{m}}$ tel que $i(K_{\mathfrak{m},1}) \subset H \subset \mathbb{I}^{\mathfrak{m}}$. Soit $h = [\mathbb{I}^{\mathfrak{m}} : H]$ l'indice de H dans $\mathbb{I}^{\mathfrak{m}}$.

Théorème 4.1.1. *Soit S un ensemble des idéaux premiers contenus dans le sous groupe H. Si S a une densité de Dirichlet alors $\delta(S) \leq \frac{1}{h}$*

Démonstration. Soit χ un caractère de $\mathbb{I}^{\mathfrak{m}}/H$, vue comme caractère de $\mathbb{I}^{\mathfrak{m}}$. Alors d'après la **Proposition**3.1.3, on déduit que

$$LogL(s,\chi) = \sum_{\mathcal{P}\nmid\mathfrak{m}} \chi(\mathcal{P})\mathcal{N}(\mathcal{P})^{-s} + g_\chi(s).$$

Où $g_\chi(s)$ est bornée en $s = 1$ ($g_\chi(s)$ est analytique pour Re(s)>1/2).
Pour chaque $\mathcal{P}$, $\sum \chi(\mathcal{P})$ pris sur tous les caractères de $\mathbb{I}^{\mathfrak{m}}/H$ est zéro, sauf pour $\mathcal{P} \in H$. Dans ce cas la somme sur les caractères est h (**Proposition**3.1.6 Orthogonalité). D'où

$$h \sum_{\mathcal{P}\in H} \mathcal{N}(\mathcal{P})^{-s} = \sum_{\chi\neq\chi_0} (LogL(s,\chi) - g_\chi(s)) + Log((s-1)L(s,\chi_0)) - Log(s-1) - g_{\chi_0}(s)$$

Par la supposition on aura

$$\sum_{\mathcal{P}\in S}\mathcal{N}(\mathcal{P})^{-s} = -\delta(S)Log(s-1)+g(s)$$

avec $g(x)\sim 0$. l'hypothèse $S\subset H$ implique que la fonction $f(s)=\sum_{\mathcal{P}\in H}\mathcal{N}(\mathcal{P})^{-s}-\sum_{\mathcal{P}\in S}\mathcal{N}(\mathcal{P})^{-s}$ est non négative lorsque s réel et $s>1$. Il s'ensuit que

$$f(s) = -(\frac{1}{h}-\delta(S))Log(s-1)+\frac{1}{h}\sum_{\chi\neq\chi_0}(Log(L(s,\chi))-g_\chi(s))+\frac{1}{h}Log(s-1)L(s,\chi_0)-\frac{1}{h}g_{\chi_0}(s)-g(s) \tag{4.1}$$

est positive lorsque s est réel et $s>1$. Toutes les fonctions notées par $g(s)$ sont bornées en $s=1$ et la même chose pour $Log((s-1)L(s,\chi_0))$ (**Proposition**3.3.1).
Le terme $LogL(s,\chi)$ est borné en $s=1$ sauf si $L(1,\chi)=0$ (Notons que $L(s,\chi)$ est continue en $s=1$ pour $\chi\neq\chi_0$), c'est à dire on peut écrire $L(1,\chi)$. Si $L(1,\chi)=0$ pour $\chi\neq\chi_0$ alors le terme Log tend vers $-\infty$ lorsque s tend vers 1. On se restreint au cas réel $s>1$ donc $Log(s-1)$ est négative lorsque s est voisinage de 1. Donc l'unique chemin pour que $f(s)>0$ peut se produire si $\delta(S)\leq\frac{1}{h}$. Aussi on a $L(1,\chi)\neq 0$ pour $\chi\neq\chi_0$. Donc la densité des premiers contenus dans H est inférieure ou égale à $1/h$. □

Proposition 4.1.1. *On garde les mêmes notations et conditions du* ***Théorème****4.1.1.*
Si $\delta(S)=\frac{1}{h}$ alors pour tout caractère non principal χ on a $L(1,\chi)\neq 0$.

Démonstration. La fonction $f(s)$ définie dans la preuve du **Théorème**4.1.1 est positive pour les réels s suffisamment proche de 1, mais le coefficient de $Log(s-1)$ est nul. Les autres coefficients sont bornés en $s=1$ et tend vers $-\infty$ si $L(1,\chi)=0$. Ce qui n'est pas vrai. □

4.2 Théorème de Densité de Frobenius

Soit K un corps de nombres et L une extension Galoisienne de K, Notons $G=\mathrm{Gal}(L|K)$

Généralités

Définition 4.2.1. Soit σ un élément d'ordre n dans G. La division de σ est l'ensemble des éléments de G qui sont conjugué à une puissance σ^m avec $\gcd(m,n)=1$

Proposition 4.2.1. *Soient σ un élément d'ordre n dans G, $H=<\sigma>$ le groupe cyclique engendré par σ et t le nombre des éléments dans la division de σ. Alors $t=\varphi(n)[G:N_G(H)]$ où $\varphi(n)$ est l'indicateur d'Euler.*

Démonstration. Pour m relativement premier à n, on a $C_G(\sigma) = C_G(\sigma^m)$ d'où σ^m admet $[G : C_G(\sigma)]$ conjugués. Comme m parcourt tous les entiers compris entre 1 et n premiers avec n. On compte $\varphi(m)[G : C_G(\sigma)]$ conjugués mais ne sont pas tous différentes. Un élément est compté q fois s'il est conjugué à q différentes puissances σ^m.
Le nombre des différentes puissances σ^m qui sont conjugués à σ est le nombre des automorphismes de H induit par conjugaison. Soit $q = [N_G(H) : C_G(\sigma)]$. Il s'ensuit que $t = \frac{\varphi(n)[G:C_G(\sigma)]}{[N_G(H):C_G(\sigma)]} = \varphi(m)[G : N_G(H)]$ □

Théorème de densité

Théorème 4.2.1. *Soit L une extension Galoisiènne d'un corps de nombres K de groupe de Galois $G = \mathrm{Gal}(L|K)$ et $\sigma \in G$ un élément ayant t éléments dans sa division. Soit S_1 l'ensemble des premiers de K divisibles par un premier de L dont l'automorphisme de Frobenius est dans la division de σ. Alors S_1 admet une densité de Dirichlet $\delta(S_1) = \frac{t}{|G|}$*

Démonstration. La preuve se fait par induction sur n, l'ordre de σ.
Considérons le premier cas $n = 1$. Alors $\sigma = 1$ et S_1 l'ensemble des premiers de K qui se décompose complètement dans L. Soit S_L l'ensemble des premiers de L divisant un premier dans S_1. Donc chaque $\mathcal{P} \in S_1$ est divisible exactement par $[L : K] = |G|$ premiers dans S_L et chacun de ces premiers est de norme exactement $\mathcal{P}$. On trouve

$$\sum_{\mathcal{B}\in S_L} \mathcal{N}_L(\mathcal{B})^{-s} = \sum_{\mathcal{B}\in S_L} \mathcal{N}_K(N_{L|K}(\mathcal{B}))^{-s} = |G| \sum_{\mathcal{P}\in S_1} \mathcal{N}_K(\mathcal{P})^{-s}.$$

Calculons la première somme :
Si S^* est l'ensemble des premiers de L ayant le degré sur $\mathbb{Q}$ est 1, alors $S^* \subset S_L$. On sait par la **Propriété**4.1.2 que $\delta(S_L) = \delta(S_L \cap S^*) = \delta(S^*) = 1$. Il s'ensuit que $|G| \sum_{\mathcal{P}\in S_1} \mathcal{N}_K(\mathcal{P})^{-s} \sim -Log(s-1)$. Donc $\delta(S_1) = \frac{1}{G}$.
Supposons que σ est d'ordre $n > 1$. pour chaque diviseur d de n, soit t_d le nombre des éléments dans la division dans σ^d. Soit S_d l'ensemble des premiers de K divisible par des premiers de L dont l'automorphisme de Frobenius appartient à la division de σ^d. Par induction on a $\delta(S_d) = \frac{t_d}{|G|}$ si $d \neq 1$.
Soit E un sous corps de L, fixé à gauche par $H =< \sigma >$. En vertu de la décomposition des premiers dans L. On a un premier $\mathcal{P}$ de K est divisible par un premier $\mathcal{B}$ de L tel que l'automorphisme d'Artin de Frobenius τ de $\mathcal{B}$ admet un cycle de longueur un, lorsque il opère par permutation sur les classes $H\gamma$ de $(G/H)_d$. Ceci est réalisé précisément lorsque $\gamma\tau\gamma^{-1} \in H$. Si cela est réalisé alors τ est conjugué à une puissance de σ et donc $\mathcal{P} \in S_d$ pour un certain d. Soit S_L l'ensemble des premiers de L ayant un degré relative 1 sur K. Pour $\mathcal{P} \in S_d$, soit

$n(\mathcal{P})$ le nombre des premiers différentes de L divisant $\mathcal{P}$ et ayant degré relative 1 sur K. Chaque $\mathcal{P} \in S_d$ est norme exactement de $n(\mathcal{P})$ premiers dans L ayant un degré un sur $\mathbb{Q}$. Donc $\delta(S_L) = 1$, car S_L contient les premiers de L ayant le degré relative 1 sur $\mathbb{Q}$

$$- Log(s-1) \sim \sum_{\mathcal{B} \in S_L} \mathcal{N}_K(N_{L|K}(\mathcal{B}))^{-s} \sim \sum_{d|n} \sum_{\mathcal{P} \in S_d} n(\mathcal{P}) \mathcal{N}_{L|\mathbb{Q}}(\mathcal{P})^{-s} \tag{4.2}$$

Précisons le nombre $n(\mathcal{P})$.
Supposons que $\mathcal{P} \in S_d$. Alors $n(p)$ est le nombre des classes $H\gamma$, $H\gamma\sigma^d = H\gamma$ [Chap3,Théorème 2.7,[1]]. Ceci est vérifié si et seulement si $\gamma\sigma^d\gamma^{-1} \in H$. Puisque H est cyclique, il peut se réaliser si $\gamma\sigma^d\gamma^{-1} \in < \sigma^d >$ en d'autre termes $\gamma \in N_G(< \sigma^d >)$. Donc on a $n(\mathcal{P}) = [N_G(< \sigma^d >) : H]$, pour $\mathcal{P} \in S_d$.
On reprend l'**Equation**4.2, et on utilise l'induction en tenant compte la somme sur S_d, $d \neq 1$ et $n(\mathcal{P})$ on obtient :

$$[N_G(H) : H] \sum_{\mathcal{P} \in S_1} \mathcal{N}_{L|\mathbb{Q}}(\mathcal{P})^{-s} \sim [-1 + \sum_{d|n,\, d \neq 1} \frac{[N_G(< \sigma^d >) : H]}{|G|} t_d] Log(s-1).$$

On a $t_d = \varphi(n/d)[G : N_G(< \sigma^d >)]$. Donc le coefficient de $Log(s-1)$ devient

$$-1 + \sum_{d|n,\, d \neq 1} \frac{1}{n} \varphi(n/d) = -1 + \frac{\varphi(n)}{n} + \frac{1}{n} \sum_{d|n} \varphi(n/d). \tag{4.3}$$

La sommation qui reste est bien connue lorsque on donne une valeur à n (le produit des polynômes cyclotomiques de degré $\varphi(n/d)$ est $X^n - 1$). donc l'expression de l'**Equation**4.3 a pour valeur $-\frac{\varphi(n)}{n}$. Enfin

$$\sum_{\mathcal{P} \in S_1} \mathcal{N}_{K|\mathbb{Q}}(\mathcal{P})^{-s} \sim \frac{-\varphi(n)}{[N_G(H) : H]n} Log(s-1) \sim -\frac{t}{|G|} Log(s-1).$$

Ce qui montre que la densité de Dirichlet de S_1 est $t/|G|$. □

Théorème 4.2.2. *Soit L une extension abélienne de K et S un ensemble fini des idéaux premiers de A_K contenant tous les idéaux ramifiés dans L. Alors l'application d'Artin $\phi_{L|K}$ envoie $\mathbb{I}^S$ sur* $\mathrm{Gal}(L|K)$.

Démonstration. Soit σ un élément de G, la division de σ consiste aux éléments qui engendre le groupe cyclique $< \sigma >$ (Car G est abelien). Par le **Théorème**4.2.1 (Théorème de la densité de Frobenius), il existe une infinité des idéaux premiers de L dont l'automorphisme de Frobenius engendre $< \sigma >$. Soit $\mathcal{B}$ un parmi ces premiers tel que $\mathcal{P} = \mathcal{B} \cap A_K$ qui n'est pas dans S, ceci

est possible car S est fini. Alors $\phi_{L|K}(\mathcal{P})$ engendre $< \sigma >$. Donc $\sigma \in \phi_{L|K}(\mathbb{I}^S)$. Or σ est choisi quelconque. D'où le résultat. □

Corollaire 4.2.1. *Soient L_1 et L_2 deux extensions de Galois de K, et soit S_i l'ensemble des premiers dans A_K qui se décomposent complètement dans L_i, pour $i = 1, 2$.*
Si $S_1 \subset S_2$ sauf pour un ensemble de densité zéro Alors $L_2 \subset L_1$

Démonstration. Supposons que $S_1 \subset S_2$, avec l'exception possible d'un ensemble de densité nulle. Soit $L = L_1L_2$, alors les premiers qui se décomposent dans L sont ceux de S_1, car ils se décomposent dans L_1 et dans L_2.
Calculons les densités de S_1 et S_2, d'après le **Théorème**4.2.1 on conclut que

$$\frac{1}{[L:K]} = \delta(S_1) = \frac{1}{[L_1:K]}$$

Ce qui efforce $L = L_1L_2 = L_1$ donc $L_2 \subset L_1$. □

Corollaire 4.2.2. *On suppose que* $\mathrm{Gal}(L|K)$ *est cyclique d'ordre n et soit d un diviseur de n. Soit S_d l'ensemble des idéaux premiers de A_K ayant exactement d facteurs dans A_L. Alors : S_d admet une densité non nulle $\frac{\varphi(n/d)}{n}$.*
En particulier, il existe une infinité de nombre premiers de A_K qui restent inerte dans A_L.

Démonstration. Un ideal premier $\mathcal{P}$ dans A_K admet d facteurs dans A_L si et seulement si $\sigma = \phi_{L|K}(\mathcal{P})$ est d'ordre n/d (sauf peut être pour l'ensemble fini des premiers qui se ramifient dans L). dans un groupe cyclique le nombre de ces éléments est $\varphi(n/d)$. par le **Théorème**4.2.1 on déduit que $\delta(S_d) = \frac{\varphi(n/d)}{n}$. □

Première inégalité fondamentale

Théorème 4.2.3. *Soient L une extension Galoisiènne de K et $\mathfrak{m}$ un module de K. Soit $\mathbb{I}_L^{\mathfrak{m}}$ le sous groupe de $\mathbb{I}_L$ engendré par tous les idéaux premiers $\mathcal{B}$ de L pour les quels $\mathcal{B} \cap K$ sont dans $\mathbb{I}_K^{\mathfrak{m}}$. Alors*

$$[\mathbb{I}_K^{\mathfrak{m}} : N_{L|K}(\mathbb{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})] \leq [L:K]$$

Démonstration. Soit $H = N_{L|K}(\mathbb{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})$. Sauf pour un nombre fini des premiers, les premiers de K qui se décomposent complètement dans L appartiennent à $N_{L|K}(\mathbb{I}_L^{\mathfrak{m}})$. La densité de cet ensemble est $\frac{1}{[L:K]}$. D'après le **Théorème**4.2.1, si h est l'indice de H dans $\mathbb{I}_K^{\mathfrak{m}}$ alors la densité des premiers qui appartient à H est $\frac{1}{h}$. Or les premiers de $N_{L|K}(\mathbb{I}_L^{\mathfrak{m}})$ sont contenus dans ceux de $N_{L|K}(\mathbb{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})$. D'où $\frac{1}{[L:K]} \leq \frac{1}{h}$, soit $[L:K] \geq h$. □

4.3 progression Arithmétique

Cette section est réservée au théorème de Dirichlet sur les premiers dans la progression Arithmétique.
Soit m un entier et $\mathfrak{m}$ le module $(m)\mathcal{P}_\infty$ pour $\mathbb{Q}$. Soit $H = i(\mathbb{Q}_{\mathfrak{m},1}) \subset \mathbb{I}_{\mathbb{Q}}^{\mathfrak{m}}$. on a $[\mathbb{I}_{\mathbb{Q}}^{\mathfrak{m}} : H] = \varphi(m)$. En effet, le sous groupe H est composé des idéaux fractionnaire (a/b) avec a,$b \in \mathbb{Z}$ premiers entre eux et $a \equiv b \bmod \mathfrak{m}$. Chaque élément de $\mathbb{I}_{\mathbb{Q}}^{\mathfrak{m}}$ à la forme $(c/d), c$,$d \in \mathbb{Z}$ et les deux sont premiers avec m. Si r est un entier fixé relativement premier à m et si les deux nombres c/d et x/y remplissent $c \equiv rd \bmod m$ et $x \equiv ry \bmod m$ alors (c/d) et (x/y) appartiennent à la même classe de $\mathbb{I}_{\mathbb{Q}}^{\mathfrak{m}}/H$. Inversement si (c/d) et (x/y) sont dans la même classe de $\mathbb{I}_{\mathbb{Q}}^{\mathfrak{m}}/H$ alors $c \equiv rd \bmod m$ et $x \equiv ry \bmod m$ où r est un entier qui satisfait $c \equiv rd \bmod m$. Il s'ensuit qu'il existe une classe dans $\mathbb{I}_{\mathbb{Q}}^{\mathfrak{m}}/H$ pour chaque classe résiduel premier à m. Donc l'indice est l'indicateur d'Euler $\varphi(m)$.
Soit β une racine primitive m^{ieme} de l'unité et $L = \mathbb{Q}(\beta)$. Or tous les idéaux de $\mathbb{Z}$ qui se décomposent complètement dans $\mathbb{Q}(\beta)$ appartiennent à H. La densité de cet ensemble est $\frac{1}{[L:\mathbb{Q}]}$ (Par **Théorème**4.2.1). Aussi par la **Proposition**4.1.1 ce nombre est au plus $\frac{1}{[\mathbb{I}_{\mathbb{Q}}^{\mathfrak{m}}:H]} = \varphi(m)$, soit $\varphi(m) \leq [L : \mathbb{Q}]$.
D'autre part β admet au plus $\varphi(m)$ conjugués, son polynôme minimal est de degré au plus $\varphi(m)$. Donc $[L : Q] = \varphi(m)$.
La connaissance de la densité des premiers dans H, qui vaut exactement $[L : \mathbb{Q}]^{-1}$, permet de formuler la conclusion suivante

Proposition 4.3.1. *Si χ un caractère non principal du groupe Quotient $\mathbb{I}_{\mathbb{Q}}^{\mathfrak{m}}/i(\mathbb{Q}_{\mathfrak{m},1})$ alors $L(1,\chi) \neq 0$.*

Théorème 4.3.1. *Soit $\mathbf{k}_0$ une classe de $\mathbb{I}^{\mathfrak{m}}$ modulo $i(\mathbb{Q}_{\mathfrak{m},1})$. Alors :*
L'ensemble des premiers dans $\mathbf{k}_0$ a pour densité $\frac{1}{\varphi(m)}$.

Démonstration. Soit χ un caractère du groupe fini $C^{\mathfrak{m}} = \mathbb{I}_{\mathbb{Q}}^{\mathfrak{m}}/i(\mathbb{Q}_{\mathfrak{m},1})$ alors :

$$LogL(s,\chi) \sim \sum_p \frac{\chi(p)}{p^s} = \sum_{\mathbf{k} \in C^{\mathfrak{m}}} \chi(\mathbf{k}) \sum_{p \in \mathbf{k}} p^{-s}. \tag{4.4}$$

Multiplions par $\chi(\mathbf{k}_0^{-1})$ et on fait la somme sur tous les caractères de $C^{\mathfrak{m}}$ on obtient

$$LogL(s,\chi_0) + \sum_{\chi \neq \chi_0} \chi(\mathbf{k}_0^{-1}) LogL(s,\chi) = \sum_{\mathbf{k}} \sum_{\chi} \chi(\mathbf{k}_0^{-1}\mathbf{k}) \sum_{p \in \mathbf{k}} p^{-s}.$$

Par l'orthogonalité on tire que $\sum_\chi \chi(\mathbf{k}_0^{-1}\mathbf{k}) = \begin{cases} \varphi(m) & \text{si } \mathbf{k} = \mathbf{k}_0 \\ 0 & \text{si } \mathbf{k} \neq \mathbf{k}_0 \end{cases}$. La somme sur les caractères non principaux dans l'**Equation**4.4 est bornée en $s = 1$, car si $\chi \neq \chi_0$ alors $L(1,\chi) \neq 0$, et on a finalement

$$LogL(s,\chi_0) \sim \varphi(m) \sum_{p \in \mathbf{k}_0} p^{-s}.$$

La représentation produit de $L(s,\chi_0)$ diffère uniquement par un nombre fini de facteurs (proviennent des premiers divisant $\mathfrak{m}$) de la représentation produit de $\zeta_{\mathbb{Q}}(s)$. On conclut que

$$LogL(s,\chi) \sim Log\zeta_{\mathbb{Q}}(s) \sim -Log(s-1).$$

Combinant les deux on trouve

$$\varphi(m) \sum_{p \in \mathbf{k}_0} p^{-s} \sim -\frac{1}{\Phi(m)} log(s-1).$$

D'où le résultat. □

Théorème 4.3.2. *Soient m un entier positive et a un entier premier à m. Alors, il existe une infinité de nombre premier de la forme $mt + a, t \in \mathbb{Z}$.*

Démonstration. Soit $\mathfrak{m} = (m)\mathcal{P}_\infty$. Soit p un premier avec $p \in a\mathbb{Q}_{\mathfrak{m},1}$. Alors $p = ax/y$ avec $x \equiv y \bmod \mathfrak{m}$. Puisque x et y sont entiers, on aura $x = y+mt$ et $p = a(y+mt)/y = a+(mt/y)$. Il s'ensuit que y divise t et donc p est la progression arithmétique des entiers congrus à a modulo m.
Inversement : Si $p = a + mk$ alors $p/a \equiv 1 \bmod m$ et $p \in a\mathbb{Q}_{\mathfrak{m},1}$, alors les premiers congrus à a mod m ont pour densité $1/\varphi(m)$. Donc il existe une infinité de ces nombres. □

Théorème 4.3.3. *Soit χ un caractère non principal de $\mathbb{I}_K^{\mathfrak{m}}/i(K_{\mathfrak{m},1})$ alors $L(1,\chi) \neq 0$.*

Démonstration. Il existe un corps de classes L du groupe idéal contenant $i(K_{\mathfrak{m},1})$ et les idéaux premiers qui se décomposent complètement dans L sont ceux de $i(K_{\mathfrak{m},1})$ sauf pour un nombre fini. La densité de ces premiers dans $i(K_{\mathfrak{m},1})$ est $\frac{1}{[L:K]}$. Par le Théorème de Frobenius, la réciprocité implique que ce nombre est $\frac{1}{[\mathbb{I}_K^{\mathfrak{m}}:i(K_{\mathfrak{m},1})]}$. On en déduit que $L(1,\chi) \neq 0$. □

Théorème de Densité de Tchebotarev

Soit $L|K$ une extension abélienne de groupe de Galois G. Chaque élément σ de G est l'image d'une unique classe modulo $\mathcal{N}(\mathbb{I}_K^{\mathfrak{m}})\, i(K_{\mathfrak{m},1})$ sous l'action de $\phi_{L|K}$.
La densité des premiers $\mathcal{P}$ de K pour les quels $\phi(\mathcal{P}) = \sigma$ est $\frac{1}{|G|}$.

Théorème 4.3.4. *Soient L une extension Galoisiènne de K de groupe de Galois G et σ un élément de G. On suppose que σ admet c conjugués dans G. Alors :*
L'ensemble des premiers de K ayant un diviseur premier dans L dont l'automorphisme de Frobenius est σ est de densité $c/|G|$.

Démonstration. Soit E le sous corps fixé par $<\sigma>$ et S' l'ensemble des premiers $\mathcal{B}$ de E pour les quels $\phi_{L|E}(\mathcal{B}) = \sigma$. On a S' est de densité $\frac{1}{\theta(\sigma)}$, ($\mathrm{Gal}(L|E) =<\sigma>$ abélien). Soit S le sous ensemble des premiers de S' ayant des degrés relatives 1 sur K. Pour $\mathcal{B} \in S$ et $\mathcal{P} = \mathcal{B} \cap K$, on détermine le nombre des premiers $\mathcal{B}_i \in S$ au dessus de $\mathcal{P}$. Dans un premier temps, soit $\mathcal{D}$ un premier de L qui divise $\mathcal{B}$ et admet σ comme son automorphisme de Frobenius sur E. Soit $<\sigma>\tau_j, j = 1, \ldots, t$ les différentes classes de $<\sigma>$ dans G. Les différentes premiers de L divisant $\mathcal{P}$ sont $\tau_j(\mathcal{D})$ et les premiers divisant $\mathcal{P}$ dans E sont $\mathcal{B}_j = \tau_j(\mathcal{D}) \cap E$. Ces derniers sont différentes, car L est Galois sur E et les premiers de L au dessus d'un même premier de E sont conjugués par un élément de $<\sigma>= \mathrm{Gal}(L|E)$. Les idéaux $\mathcal{B}_i$ ont un degré relative un sur K si et seulement si $<\sigma>\tau_j\sigma =<\sigma>\tau_j$ si et seulement si $\tau_j\sigma\tau_j^{-1} \in <\sigma>$, (Voir chapitre 3, proposition 2.7[1]). Supposons que cela est vrai alors

$$\phi_{L|E}(\mathcal{B}_j) = \left(\frac{L|E}{\tau_j(\mathcal{D})}\right) = \tau_j \left(\frac{L|E}{\mathcal{D}}\right) \tau_j^{-1}.$$

Il s'ensuit que $\mathcal{B}_j \in S$ si et seulement si $\sigma = \tau_j\sigma\tau_j^{-1}$, où $\tau_j \in C_G(\sigma)$.
Le nombre des premiers dans S divisant $\mathcal{P}$ est $d = [C_G(\sigma) :<\sigma>]$.
Si T l'ensemble des premiers de K divisible par un premier de S. Pour chaque $\mathcal{P} \in T$, il existe exactement d premiers $\mathcal{B} \in S$ pour les quels $N_{E|K}(\mathcal{B}) = \mathcal{P}$. En termes de densité ceci signifie $d\delta(T) = \delta(s) = \frac{1}{|G|}$. Finalement $\delta(T) = \frac{1}{d}\frac{1}{\Theta(\sigma)} = \frac{1}{|C_G(\sigma)|} = \frac{c}{|G|}$. □

Bibliographie

[1] G. J. Janusz, *Algebraic Number Fields (Second edition).* Volume 7, American Mathemtical Society, (1996).

[2] E.C. Titchmarsh, *The Theory of The Riemann Zeta-Function.* Clarendon Press. Oxford, 1951.

[3] J.S. Meline, *Algebraic Number Theory (V3. 03).* www.jmlne.org/math, 2011.

[4] H.M. Stark, *A complete determination of complex quadratic fields of class number one,* Moch. Math J. 14 (1967),1-27.

[5] S. Alaca, K. Williams, *Introductory Algebric number theory.* (Carleton university, Ottawa), (2004).